

Volume Four

Aviation Security

CAI
ZI
-2006
I11

V. 4

Air India Flight 182 A Canadian Tragedy

Commission of Inquiry
into the Investigation
of the Bombing of
Air India Flight 182





Digitized by the Internet Archive
in 2024 with funding from
University of Toronto

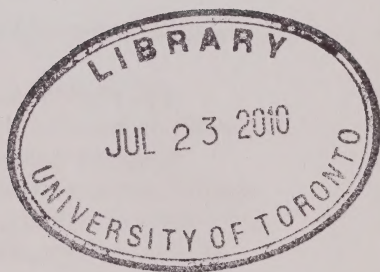
<https://archive.org/details/39300917040221>

Air India Flight 182

A Canadian Tragedy

VOLUME FOUR

Aviation Security



©Her Majesty the Queen in Right of Canada, represented by the
Minister of Public Works and Government Services, 2010

Cat. No: CP32-89/2-2010E

ISBN: 978-0-660-19926-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943

Fax: (613) 954-5779 or 1 800 565-7757

Publications@pwgsc.gc.ca

Internet: www.publications.gc.ca

VOLUME FOUR AVIATION SECURITY

TABLE OF CONTENTS

CHAPTER I: INTRODUCTION

CHAPTER II: RESPONSES TO THE BOMBING OF AIR INDIA FLIGHT 182

2.1	International Response	15
2.1.1	International Air Transport Association	15
2.1.2	International Civil Aviation Organization	18
2.1.3	United States: Federal Aviation Administration	21
2.1.4	Ireland: Coroner's Inquest	22
2.1.5	India: Kirpal Commission	23
2.2	Canadian Response	26
2.2.1	Introduction	26
2.2.2	1985 Airport Security Audit	30
2.2.3	Seaborn Report	32
2.2.4	Canadian Aviation Safety Board Investigation	36
2.2.5	Changes to Legislative and Regulatory Framework	37
2.2.6	Changes in Oversight	39
	2.2.6.1 <i>Roles and Responsibilities</i>	39
	2.2.6.2 <i>Inspection and Enforcement</i>	39
2.2.7	Changes in Training	41
2.2.8	Enhancements in Security Systems and Equipment	42
2.2.9	Conclusion	42
2.3	Failure to Learn: The Bombing of Pan Am Flight 103	44
2.3.1	Failure to Address the Known Threat of a Bomb in Interlined, Unaccompanied Baggage	45
2.3.2	Air India and Pan Am: Parallel Systemic Failures	51
2.3.3	Responses to the Bombing of Pan Am Flight 103	54
2.3.4	Failure to Appreciate Significance of Air India Flight 182 Bombing	58
2.3.5	Conclusion	61

CHAPTER III: CIVIL AVIATION SECURITY IN THE PRESENT DAY

3.1	Responses to the Terrorist Attacks of September 11, 2001	63
3.1.1	Historical Context	63

3.1.2	International Response	65
3.1.2.1	<i>International Civil Aviation Organization: Annex 17 Amendments</i>	66
3.1.2.2	<i>International Civil Aviation Organization: Universal Security Audit Program</i>	68
3.1.2.3	<i>North America</i>	76
3.1.2.4	<i>Europe</i>	77
3.1.3	Canadian Response	77
3.1.3.1	<i>Introduction</i>	77
3.1.3.2	<i>Canadian Air Carrier Protective Program</i>	82
3.1.3.2.1	<i>Genesis and Development of the CACPP</i>	76
3.1.3.2.2	<i>Threat Matrix</i>	83
3.1.3.2.3	<i>Role of Aircraft Protective Officers In-Flight Security Airport Security Behavioural Analysis Intelligence</i>	84
3.1.3.2.4	<i>Criticism of Air Marshal Programs</i>	88
3.1.3.2.5	<i>APO Recruitment, Training and Retention</i>	90
3.1.3.2.6	<i>Flight Crew Training</i>	92
3.1.3.2.7	<i>International Cooperation</i>	92
3.1.3.2.8	<i>Funding</i>	93
3.1.3.2.9	<i>Need for the Program</i>	93
3.1.4	After 9/11: Danger of Complacency Continues	94
3.1.5	Conclusion	95
3.2	Oversight in Aviation Security	96
3.2.1	International Governance	99
3.2.1.1	<i>International Regulatory Regime</i>	99
3.2.1.1.1	<i>International Conventions</i>	102
3.2.1.1.2	<i>Annex 17 and the ICAO Security Manual</i>	106
3.2.1.2	<i>Limitations on International Governance</i>	111
3.2.2	Oversight of Aviation Security in Canada	116
3.2.2.1	<i>Concepts in Oversight</i>	120
3.2.2.2	<i>Oversight of Aviation Security</i>	120
3.2.2.2.1	<i>Annex 17 and Canadian Aviation Security Regulatory Framework National Civil Aviation Security Program and Stakeholder Security Programs National Aviation Security Committee and Stakeholder Security Committees</i>	121
3.2.2.2.2	<i>Regulatory Regime Underlying Principles</i>	130

	<i>Proactive Approach</i>	
	<i>Layered Approach</i>	
	<i>Performance-based Approach</i>	
	<i>Security Culture and Risk Management</i>	
	<i>Identifying Threats: Past, Present and Future</i>	
3.2.2.2.3	<i>Inspection and Enforcement</i>	141
3.2.2.2.4	<i>Shared Responsibility: Role of Stakeholders in Oversight</i>	142
3.2.2.2.5	<i>Independent Reviews of Aviation Security</i>	143
3.2.3	<i>Conclusion</i>	146
3.3	<i>Risk Management in Aviation Security</i>	147
3.3.1	<i>Risk Management: Introduction</i>	148
3.3.2	<i>Risk Management in Aviation Security</i>	150
3.3.3	<i>Risk Management Methodology</i>	155
3.3.4	<i>Risk Management Decision-making in Practice</i>	160
3.3.5	<i>Matching Limited Resources with Risk Control Objectives</i>	172
3.3.6	<i>Shared Responsibility and Accountability</i>	174
3.3.7	<i>Culture of Security</i>	179
3.3.8	<i>Conclusion</i>	181
3.4	<i>Use of Intelligence in Aviation Security</i>	181
3.4.1	<i>Integrated Threat Assessment Centre</i>	183
3.4.2	<i>Information Sharing: Canadian Air Transport Security Authority</i>	184
3.4.3	<i>Information Sharing: Aviation Security Partners</i>	186
3.4.4	<i>Conclusion</i>	190
3.5	<i>Passenger and Baggage Screening</i>	191
3.5.1	<i>Post-1985 Developments</i>	192
3.5.1.1	<i>Hold Bag Screening</i>	192
3.5.1.2	<i>Creation of the Canadian Air Transport Security Authority</i>	195
3.5.2	<i>Passenger and Baggage Security: Lessons Yet to be Learned</i>	198
3.5.2.1	<i>Need for Proactive Approach</i>	198
3.5.2.2	<i>Holistic Security: "Single Entity" Doctrine</i>	201
3.5.3	<i>Passenger and Baggage Screening: Current Procedures and Future Developments</i>	203
3.5.3.1	<i>Hold Bag Screening and Passenger-Baggage Reconciliation</i>	203
3.5.3.2	<i>Pre-Board Screening</i>	205
3.5.3.2.1	<i>Identity Screening Initiatives</i>	207
	<i>Advance Passenger Information and Passenger Name Record</i>	
	<i>Trusted Traveller Programs</i>	
	<i>Behavioural Analysis</i>	
	<i>Passenger Protect Program</i>	

	<i>Rationale for the Program</i>	
	<i>Advisory Group and Specified</i>	
	<i>Persons List</i>	
	<i>Reconsideration Process</i>	
	<i>Consequences of Boarding Denials</i>	
	<i>Balancing Security and Rights</i>	
	<i>Regulatory Amendments</i>	
3.5.4	Conclusion	233
3.6	Use of Technology	234
3.6.1	Technology and Pre-board Screening	234
3.6.1.1	Dual Energy X-ray	235
3.6.1.2	Threat Image Projection Systems	236
3.6.1.3	Explosives Detection Trace and Explosives Vapour Detection Systems	
3.6.1.4	Closed-Circuit Television Monitoring	237
3.6.2	Technology and Hold Bag Screening	238
3.6.2.1	Canada's Five-level HBS System	238
3.6.2.2	CT X-ray Systems	240
3.6.3	Access Control	240
3.6.3.1	Biometrics	240
3.6.4	Technology: Concerns and Limitations	242
3.6.4.1	Privacy and Safety Issues	243
3.6.4.2	Reliability	244
3.6.5	Other Screening Systems	246
3.6.5.1	Passenger-Baggage Reconciliation	246
3.6.5.2	Explosives Detection Dogs	247
3.6.6	Conclusion	248
3.7	Screeners	249
3.7.1	Recruitment	250
3.7.2	Training	254
3.7.3	Turnover	259
3.7.4	Testing	261
3.7.5	Conclusion	266
3.8	Closing the Gaps in Aviation Security	266
3.8.1	Air Cargo	266
3.8.1.1	Air Cargo Security: A Decades-old Concern	270
3.8.1.1.1	The Seaborn Report	273
3.8.1.1.2	Reasons for Inaction	276
3.8.1.1.3	Need for a Proactive Approach	278
3.8.1.2	International Developments in Air Cargo Security	279
3.8.1.2.1	The Problem: Cargo Consignments can Target Specific Aircraft	280
3.8.1.2.2	The Proposed Solution: "Known Shipper"	281
3.8.1.3	Canada's Existing Air Cargo Security Regime	283
3.8.1.3.1	Lack of Vigilance: "Known Shipper" Misconstrued	283
3.8.1.3.2	Canada Falls Behind	287

3.8.1.3.3	<i>Voluntary Programs</i>	288
3.8.1.3.4	<i>Inadequate Cargo Screening</i>	290
	<i>Note on Terminology</i>	
	<i>Minimal Searching of Air Cargo</i>	
	<i>Lack of Technological Equipment</i>	
	<i>Challenges in Searching Air Cargo</i>	
	<i>Lagging Technological Advancement</i>	
	<i>Explosives Detection Dogs</i>	
	<i>Working Toward a Cargo Screening Standard</i>	
	<i>Interim Measures</i>	
3.8.1.3.5	<i>Inadequate Training</i>	300
3.8.1.3.6	<i>Poor Access Control</i>	301
3.8.1.3.7	<i>Enhancements Required</i>	302
3.8.1.4	<i>Proposal for an Enhanced Regime: Air Cargo Security Initiative</i>	302
3.8.1.4.1	<i>Developments in Air Cargo Security in the United States</i>	304
3.8.1.4.2	<i>Hardening Supply Chain Security</i>	
	<i>Supply Chain Security Program</i>	
	<i>Oversight and Compliance</i>	
	<i>Monitoring</i>	308
3.8.1.4.3	<i>Improving Air Cargo Screening: Use of Technology</i>	316
3.8.1.4.4	<i>Funding</i>	322
3.8.1.5	<i>A Call for Action from the Government of Canada</i>	325
3.8.1.6	<i>Conclusion</i>	329
3.8.2	<i>Airport Security</i>	330
3.8.2.1	<i>Air India Flight 182: Airport Security Deficiencies Revealed</i>	332
3.8.2.2	<i>Basic Principles</i>	335
3.8.2.3	<i>Air Terminals as Targets of Opportunity</i>	336
3.8.2.4	<i>The Price of Poor Access Control</i>	340
3.8.2.5	<i>Access Control at Canadian Airports</i>	345
3.8.2.5.1	<i>Supervision of Non-Security Cleared Individuals</i>	356
3.8.2.5.2	<i>Restricted Area Identification Card</i>	356
3.8.2.5.3	<i>Instilling a Culture of Security</i>	
	<i>Awareness Airport Security Watch Program</i>	359
3.8.2.6	<i>Conclusion</i>	361
3.8.3	<i>Fixed Base Operations and General Aviation</i>	362
3.8.3.1	<i>Enhancing Security and Meeting the Needs of Industry</i>	368
3.8.3.2	<i>Transport Canada: Action Taken but More Required</i>	369

3.8.3.3	<i>Conclusion</i>	371
3.9	Duty to Warn and Transparency in Aviation Security	371
3.9.1	Public Warning System for Security Threats against Airlines	373
3.9.2	Informing the Public: Greater Transparency Required in Civil Aviation Security	378
3.9.3	Conclusion	384
3.10	Funding Aviation Security	385
3.10.1	Cost-Effective Security: Reasonable Balance, Flexibility and a Risk Management Approach	385
3.10.2	Sustainable Funding	393
3.10.3	Conclusion	397

EPILOGUE	398
-----------------	-----

CHAPTER IV: RECOMMENDATIONS

APPENDICES

Appendix A	417
Chronology: Significant Acts of Unlawful Interference with Civil Aviation	
Appendix B	441
Report on Security Arrangements Affecting Airports and Airlines in Canada [“Seaborn Report”]: Principal Recommendations of the Airport/Airline Security Report	
Appendix C	443
The Myth of Security At Canada’s Airports: Report of the Standing Senate Committee on National Security and Defence – Recommendations	
Appendix D	449
Flight Plan: Managing the Risks in Aviation Security – Report of the Advisory Panel – List of Recommendations	
Appendix E	457
Canadian Security Guidebook 2007 Edition: Airports – Appendix III Index of New Recommendations	

VOLUME FOUR

AVIATION SECURITY

CHAPTER I: INTRODUCTION

The terms of reference for the Commission require the Commissioner to make findings and recommendations with respect to "...whether further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, particularly those relating to the screening of passengers and their baggage."¹

Despite knowledge of existing threats and of the need for protective security measures, Canada was ill-prepared to defend itself against aviation terrorism in 1985. The bombing of Air India Flight 182 on June 23, 1985, revealed major shortcomings in the country's aviation security regime. Although Canada responded immediately and has since made numerous improvements to security, many deficiencies exposed in the wake of the bombing remain unaddressed.

It became clear to the Commission early on in its work that a broad interpretation of this aspect of its mandate was required. Although the bombing resulted directly from an unaccompanied bag that infiltrated the airline system and was then interlined to the Air India flight in Toronto, a narrow focus by the Commission on passenger and baggage security would not have provided assurance that all the security deficiencies that led to the bombing had been examined. Breaches in aviation security do not often occur in isolation. The security deficiencies that led to the bombing were widespread and interdependent, ranging from poor threat communication to lax aircraft and airport security.²

Aircraft and airport environments are attractive targets for terrorists because they offer the potential of a large number of victims in a contained area, along with a virtual guarantee of widespread public attention after an attack. Air travel is comparatively safe, since aircraft have one of the lowest accident rates of any mode of transportation.³ Nevertheless, when accidents or terrorism incidents occur, the consequences can be profound and their high visibility generates much public concern. Terrorists specifically target civil aviation because they have expectations of a high propaganda return from a successful attack.⁴

¹ Terms of Reference, P.C. 2006-293, para. b(vii).

² See Volume Two: Part 1, Pre-Bombing, Sections 1.9, 2.4, 4.3, 4.4 and 4.7 for a detailed analysis of the security breaches associated with the bombing of Air India Flight 182.

³ Exhibit P-169, p. 15 of 202.

⁴ Exhibit P-169, p. 15 of 202.

Since the 1960s, aviation has witnessed an increase in the deadliness of terrorist attacks, from simple aircraft seizures with the purpose of escaping political oppression in the 1960s to the use of aircraft as guided missiles in suicide attacks, as on September 11, 2001. Included on this continuum was the era of sabotage involving the unaccompanied, infiltrated bag – the *modus operandi* of the Air India bombers.

A careful examination of the history of civil aviation security reveals patterns that experts say give predictability to air terrorism. As Rodney Wallis, one of the Commission's key experts in civil aviation security, observed, "...There is very little that is new in threat[s] or in aviation security generally. What is changing is the ability to respond."⁵

In many ways, civil aviation security in Canada has made great strides since 1985. A stronger regulatory regime and oversight mechanism exist today. Threat communication and screening technology have vastly improved and a new government agency, the Canadian Air Transport Security Authority (CATSA), has been established exclusively to screen passengers, their baggage and non-passengers seeking access to restricted areas of airports. Still, important security deficiencies remain, despite recognition of these very deficiencies in the immediate aftermath of the bombing of Air India Flight 182.

As suggested by Wallis, the Commission has not found many new weaknesses in civil aviation security, but the fact that many deficiencies persist more than two decades after they first surfaced is of great concern. Earlier reviews of civil aviation security in Canada, notably those of the Standing Senate Committee on National Security and Defence (Senate Committee) and an independent review panel, the *CATSA Act Review Advisory Panel* (CATSA Advisory Panel), also called attention to many of these deficiencies,⁶ but they remain unaddressed.

Specifically, the Commission learned that there are several methods of sabotage besides those involving passengers and baggage. One of the most significant vulnerabilities is air cargo, which, though largely unscreened, travels in the hold of passenger aircraft.⁷ Persons and vehicles accessing airside and restricted areas of airports are also inadequately screened.⁸ In addition, the General Aviation (GA) sector and Fixed Base Operations (FBOs) have not been designated for CATSA screening. As a consequence, some passengers and their baggage are not screened at all, and the facilities used by the GA sector and FBOs are often not well secured. Flights from these facilities sometimes land at one of 89 "designated" airports in Canada, and their passengers may then transfer to connecting flights without ever being screened. In addition, a number of FBOs are located at the periphery of designated airports and permit direct access to restricted areas that normally require passing through levels of security

⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5009.

⁶ See Exhibits P-169, P-171 and P-172; see also Appendices C, D and E for a listing of the recommendations of these reports.

⁷ See Section 3.8.1, which provides a detailed analysis of the current deficiencies in air cargo security.

⁸ See Section 3.8.2, which provides a detailed analysis of the current deficiencies in airport security.

screening that FBOs do not offer.⁹ These security weaknesses in the GA sector and FBOs leave the aviation system as a whole vulnerable to attack. Bombs can still find their way onto passenger aircraft.

A key lesson of the Air India bombing is that security measures must be applied in mutually reinforcing layers that address all vulnerabilities. Each layer on its own is not foolproof, as no measure on its own can ever be. Redundancy helps ensure that, if one measure fails, another will cover the gap. Effective security requires that all gaps be covered.

In 1985, the Government of Canada itself recognized that a broad-based examination of aviation security was required in response to the bombing. Shortly after, the Government commissioned a comprehensive review, which resulted in the “Seaborn Report.” In many respects, this report is as relevant today as it was in 1985. It recommended sweeping changes to aviation security to better manage the threat of sabotage. Transport Canada implemented some, but not many, of the report’s recommendations.¹⁰ Many weaknesses identified in the Seaborn Report are now the focus of this volume of the Commission’s own report.

Annex 17 to the *Convention on International Civil Aviation* (“Chicago Convention”), a treaty governing civil aviation, outlines the minimum security standards.¹¹ As a signatory, Canada is obliged to comply with the Convention, but the Commission finds that it has not done so.

Besides calling for a multi-layered, holistic approach to security, aviation security experts and officials from Transport Canada identified several other underlying principles to strengthen defences against terrorists. Many of these principles are rooted in the lessons learned from the bombing of Air India Flight 182. Security measures must be developed to anticipate threats,¹² provide for flexibility and performance-based measures where suitable,¹³ and foster a culture of security awareness. The security regime must be constantly scrutinized for its effectiveness. Since there are few security measures available to prevent harm once an aircraft is aloft, effective security must be provided on the ground. As well, technology, even if properly used, should rarely be seen as the final answer. It is merely one tool that may assist in providing security.

Transport Canada reported that it is developing proposals to address many of the security gaps that were the focus of the Commission – primarily air cargo security, airport security and FBO and GA security. It has also undertaken a comprehensive review of its regulatory regime. The Commission strongly urges

⁹ See Section 3.8.3, which provides a detailed analysis of the current deficiencies at FBOs and in the GA sector.

¹⁰ Exhibit P-101 CAF0039; see also Appendix B, which provides a list of the recommendations.

¹¹ International Civil Aviation Organization (ICAO), *Convention on International Civil Aviation* (“Chicago Convention”), 7 December 1944, (1994) 15 U.N.T.S. 295; Exhibit P-181.

¹² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4646.

¹³ Exhibit P-169, +pp. 92-93 of 202.

Transport Canada to ensure that it honours all of its Annex 17 obligations, and to exceed them where possible by looking to international best practices. Almost 25 years after the bombing of Air India Flight 182, the time for reflection is long past. Action is now required.

There is also a need for independent oversight of security measures. For this reason, the Commission recommends a regular five-year review by an independent panel of experts to ensure that Canada is addressing threats as effectively as possible. The Commission strongly encourages the Senate Committee and the Auditor General of Canada to continue to inform the public about the state of civil aviation security in Canada.

The Commission was greatly assisted in its work, not only by the members of the independent CATSA Advisory Panel, the Senate Committee, including its Chair, Senator Colin Kenny, and the Auditor General of Canada, but also by members of the Office of the Privacy Commissioner of Canada, including the Privacy Commissioner, Jennifer Stoddart, and the many industry representatives and Transport Canada officials who appeared at the hearings. The Commission extends its thanks as well to its civil aviation security experts, including Moses Aléman, Dr. Peter St. John and Dr. Kathleen Sweet, and its expert in risk management, Dr. William Leiss, who assisted in navigating this technical field. The Commission wishes to extend its deep gratitude, in particular, to Rodney Wallis, whose knowledge and expertise in civil aviation security provided essential guidance throughout the hearings and during the preparation of this volume.

VOLUME FOUR

AVIATION SECURITY

CHAPTER II: RESPONSES TO THE BOMBING OF AIR INDIA FLIGHT 182

In the early morning of June 23, 1985, Air India Flight 182 was on its way from Toronto to London, England,¹ when a bomb exploded on board. The aircraft, a Boeing 747 named the *Kanishka*, crashed in the Atlantic Ocean off the southwest coast of Ireland, killing all 329 passengers and crew.² The bomb had been concealed in a suitcase that began its journey on Canadian Pacific Airlines (CP Air) Flight 060 from Vancouver and was later transferred to the Air India aircraft in Toronto.³ Throughout its entire transport, the suitcase containing the bomb was not accompanied by any corresponding passenger.⁴ Less than an hour before Flight 182 disappeared, another bomb hidden in a suitcase exploded in the baggage handling area of Narita Airport in Japan, killing two baggage handlers and injuring four others. This suitcase had also travelled unaccompanied from Vancouver – in this case, on CP Air Flight 003 – and was destined for loading onto Air India Flight 301 to Bangkok.⁵

The bombing of Air India Flight 182 marked a watershed in international civil aviation security.⁶ There had been incidents of aircraft sabotage before, but the scale of destruction in 1985 was unprecedented. This was also the first time that a specific *modus operandi* was identified. An unaccompanied bag had entered the airline system and was subsequently interlined to the target aircraft in a different city.⁷

Until the events of September 11, 2001, the bombing of Air India Flight 182 was the worst act of air terrorism the world had seen.⁸ It remains Canada's worst encounter with terrorism.⁹ Before the bombing, Canada's non-controversial international roles had bred complacency within Transport Canada's Civil Aviation Security Branch.¹⁰ No known terrorist group harboured grievances

¹ The flight made a transit stop in Montreal: Exhibit P-35, p. 1.

² Exhibit P-164, p. 1.

³ Exhibit P-157, p. 11 of 135.

⁴ Exhibit P-157, pp. 25, 77 of 135.

⁵ Exhibit P-157, p. 11 of 135.

⁶ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4288.

⁷ Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4209-4210; see also Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4517.

⁸ Exhibit P-35, p. 1.

⁹ Exhibit P-35, p. 2.

¹⁰ Exhibit P-157, p. 54 of 135; see also Exhibit P-259: Rodney Wallis, *Combating Air Terrorism* (New York: Brassey's, 1993), p. 7 [Wallis, *Combating Air Terrorism*].

against Canada¹¹ and, despite indications to the contrary,¹² there was a tendency to believe the country immune to the violent regional conflicts that had elsewhere led to a rash of hijackings and other forms of air terrorism.¹³ As a result, civil aviation security was given low priority.¹⁴

The bombing of Flight 182 was the result of a conspiracy that was conceived, planned and executed in Canada, and most of the victims were Canadians.¹⁵ It demonstrated that terrorist acts need not be confined to the country that was the source of a dispute, but could be perpetrated anywhere that suited terrorist purposes.¹⁶

To that point, Canada had failed to keep pace with the realities of air terrorism. The Air India bombing led to significant changes in Canadian and international civil aviation security regimes. The focus quickly shifted from preventing hijackings to preventing sabotage, particularly the threat of explosive devices hidden in checked baggage.¹⁷ A number of post-bombing investigations and reviews in Canada and abroad recommended sweeping changes to existing aviation security systems. Chief among the changes then made in Canada was the introduction of passenger-baggage reconciliation, a measure that had already been used here, and that, had it been used in June 1985, might well have prevented the Air India bombing. In the aftermath, Canada became the staunchest proponent of passenger-baggage reconciliation, leading the way for this measure to become a mandatory international civil aviation security standard. The basic security philosophies that were established following the bombing form the foundation of security regimes today.¹⁸

However, despite these efforts to enhance security, it remained inadequate. The Air India bombing revealed significant weaknesses, not only in passenger and baggage security, but in almost all areas of aviation security. Reviews of the disaster recognized that passenger aircraft were exposed to multiple methods of terrorist attack, and outlined a clear vision for comprehensive change. The Seaborn Report, commissioned by the Government of Canada in 1985, provided a strategic plan whose principles remain relevant.¹⁹ Nevertheless, the focus of the response in Canada and internationally was on passenger and baggage security. Although attempts were made to address other areas of vulnerability, they were not adequate. It was not until Pan American World Airways (Pan Am) Flight 103 was destroyed more than three years later, using the same method employed against Air India, that a greater commitment to reform in security emerged. Efforts to secure reform were further strengthened following the attacks of September 11, 2001. Still, many lessons of the Air India bombing remain unheeded almost 25 years later.

¹¹ Wallis, *Combating Air Terrorism*, p. 7.

¹² Exhibit P-157, pp. 47-48 of 135.

¹³ Exhibit P-157, p. 54 of 135.

¹⁴ Exhibit P-157, p. 54 of 135.

¹⁵ Exhibit P-35, p. 2.

¹⁶ Wallis, *Combating Air Terrorism*, p. 7.

¹⁷ Exhibit P-157, p. 75 of 135.

¹⁸ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4219.

¹⁹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4507.

2.1 International Response

The international civil aviation security community responded within days of the loss of Air India Flight 182. The International Civil Aviation Organization (ICAO) called a special meeting of its assembly. The International Air Transport Association (IATA) convened an extraordinary meeting of its Security Advisory Committee (SAC).²⁰ The SAC was a special security body of IATA established in 1967 to develop collective airline policies for combatting aviation terrorism.

Although there was no initial confirmation that a bomb had destroyed Flight 182, suspicion ran high. Given the nature of the incident and the connection to the Narita bombing, the working assumption was that a bomb had brought down Flight 182. Both incidents involved a non-existent passenger, the same airline was targeted, physical evidence of a bomb was discovered at Narita Airport,²¹ and those participating in the search and recovery process for Air India Flight 182 had observed catastrophic damage. On this basis, those attending the meetings at IATA and ICAO recommended major reforms to civil aviation security to reduce the risk of sabotage.²² Canada played a prominent role, leading the push for mandatory passenger-baggage reconciliation.²³

2.1.1 International Air Transport Association

IATA is the trade association for international scheduled airlines.²⁴ On June 28, 1985, airline security chiefs from around the world,²⁵ including representatives of Air India, CP Air and Air Canada, assembled at IATA's headquarters in Montreal to attend the SAC meeting. The measures recommended by the SAC became mandatory after the full membership adopted resolutions.²⁶

The SAC meeting was convened to review the recent aviation terrorism events and to identify immediate steps to close security gaps.²⁷ The attendance of airline representatives from around the world only days after the Air India bombing reflected the deep concern of the industry.²⁸ The airlines sought to restore public confidence, which had been "badly shattered by the incidents,"²⁹ and to maintain the viability of their operations.³⁰ A number of observers also

²⁰ Wallis, *Combating Air Terrorism*, p. 5.

²¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4483.

²² Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4482-4483.

²³ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4755.

²⁴ Wallis, *Combating Air Terrorism*, p. 102.

²⁵ The extraordinary meeting included representatives from the following airlines: CP Air, Air India, Swiss Air, KLM, TWA, Qantas, Air France, UTA, Middle East Airlines, Japan Airlines, Aer Lingus, Nigeria Airways, British Caledonian, South African Airways and British Airways. The meeting was also attended by representatives of the International Civil Aviation Organization (ICAO) and the Air Transport Association of Canada. See Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4474-4475.

²⁶ Exhibit P-260: Rodney Wallis, *Lockerbie: The Story and the Lessons* (Westport, Conn.: Praeger Publishers, 2001), pp. 4-5 [Wallis, *Lockerbie*].

²⁷ Wallis, *Combating Air Terrorism*, pp. 5-6.

²⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4475.

²⁹ Wallis, *Combating Air Terrorism*, p. 6.

³⁰ Wallis, *Combating Air Terrorism*, p. 6.

attended the IATA meeting, including representatives of Transport Canada and the US Federal Aviation Administration (FAA). The presence of government representatives at an “airline meeting” demonstrated the significance attached to the issues being discussed.³¹ The holding of the meeting so soon after the bombing permitted IATA to learn the industry’s immediate reaction and to represent its views shortly afterwards at ICAO’s special meeting.³²

Notably absent from the SAC meeting, however, were security representatives from the US airlines. According to Rodney Wallis, Director of Security at IATA at the time, officials from American air carriers viewed the bombing as a “foreign” matter that held little relevance for their operations.³³ They were focusing instead on another incident unfolding at the same time involving an American aircraft. A Trans World Airlines (TWA) Boeing 727 had been hijacked in the Mediterranean region on June 14, 1985, resulting in a two-week hostage-taking and the killing of one American passenger.³⁴ This was a major event in the US, with daily coverage in the media. Because American hostages were being held, “...the level of emotion created in the United States was certain to give precedence of thought in that country to this criminal act rather than to the Air India disaster.”³⁵ The relative inattention of US airline representatives to the lessons of the Air India bombing was to have grave repercussions three years later when, according to Wallis, Pan Am Flight 103 was bombed after the airline abandoned the key preventive measure developed following the Air India bombing.³⁶

The SAC meeting in June 1985 resulted in a number of recommendations for IATA’s membership and marked the beginning of “massive changes”³⁷ in aviation security around the world. The most significant was passenger-baggage reconciliation³⁸ – the process of matching passengers with their baggage to prevent unaccompanied bags being carried on aircraft.³⁹ To avoid the danger that arose when ill-intentioned passengers voluntarily separated themselves from their baggage, it became necessary to treat the passenger and accompanying baggage as a single entity. It was not sufficient simply to identify “no shows” at the gate, or missing transit and transfer passengers. Bags that had illegally “infiltrated” the system had to be identified.⁴⁰

Passenger-baggage reconciliation was an established procedure even before the Air India bombing. Some countries, including Spain and Turkey, had implemented fairly rudimentary passenger-baggage reconciliation procedures,

31 Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4474-4475.

32 Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4475-4476.

33 Wallis, *Lockerbie*, p. 10.

34 Wallis, *Lockerbie*, p. 10.

35 Wallis, *Lockerbie*, p. 10.

36 Wallis, *Lockerbie*, p. 11.

37 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4476.

38 Wallis, *Lockerbie*, pp. 10-11.

39 Wallis, *Lockerbie*, p. 152.

40 Wallis, *Lockerbie*, p. 13.

mostly on an *ad hoc* basis in response to bomb threats.⁴¹ Passenger-baggage reconciliation had been used successfully in Canada by KLM and CP Air in relation to a bomb threat in 1984.⁴² After the Air India bombing, the goal was to ensure that such procedures became mandatory, that they were enhanced, where applicable, through a process of automation and that the procedures were workable for both developed and developing nations.⁴³ Wallis described the mandatory requirement for passenger-baggage reconciliation as the most significant change in international civil aviation security standards during the 1980s.⁴⁴

The SAC identified additional security issues that needed greater attention, including ramp and air cargo security. Air cargo, in particular, was known to be susceptible to sabotage, and there was increasing concern about the ability to use devices hidden in air cargo to target specific aircraft. IATA established working groups of aviation security experts to review these vulnerabilities⁴⁵ and to review the ICAO Security Manual.⁴⁶ The groups reported at the next regular SAC meeting in September 1985, essentially confirming the SAC's initial views about where improved security was required.⁴⁷

Those attending the SAC extraordinary meeting gave priority to implementing controls over checked baggage,⁴⁸ but a proposal to screen all checked baggage did not find favour.⁴⁹ This measure had been strongly advocated by Transport Canada.⁵⁰ As an adjunct to passenger-baggage reconciliation, it would enhance passenger security.⁵¹ After the bombing, airlines at Canadian airports had been instructed to conduct full checked baggage screening for all international flights through physical or X-ray inspection.⁵² However, this caused considerable delays, with opportunity costs estimated at \$10,000 to \$18,000 per hour in 1985 dollars.⁵³ The SAC supported other measures instead, calling for improved communication and intelligence⁵⁴ and enhanced security at airports. IATA eventually established minimum criteria for securing airports against terrorism and inaugurated a corresponding program of airport surveys.⁵⁵

41 These procedures consisted of passengers physically identifying their baggage before it was loaded on the aircraft. See Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4412-4413, 4478.

42 Exhibit P-101 CAF0637, pp. 18-19.

43 Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4476, 4478, 4485-4486.

44 Wallis, *Lockerbie*, p. 10.

45 See Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4477, 4480.

46 Exhibit P-162, p. 4.

47 Exhibit P-162, p. 5.

48 Exhibit P-162, pp. 3, 5.

49 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4481.

50 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4481.

51 Wallis, *Lockerbie*, p. 154.

52 Exhibit P-263, Tab 13, p. 2 of 4. Note, however, that X-ray screening was still considered a cosmetic security measure that was of limited use for detecting bombs in baggage. See Wallis, *Lockerbie*, p. 12.

53 These figures were in relation to wide-bodied jets: Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4482.

54 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4481.

55 Exhibit P-157, p. 89 of 135.

While IATA is influential in the international civil aviation community, its mandate is to represent the commercial concerns of its membership, international scheduled airlines. Its recommendations represent best practices but do not have the force of law.⁵⁶ Nevertheless, IATA and ICAO have always enjoyed a co-operative relationship. In 1985, on behalf of IATA, Wallis brought the concept of passenger-baggage reconciliation – an airline proposal – to the subsequent ICAO deliberations on the Air India bombing,⁵⁷ and ICAO “...ran with this idea.”⁵⁸

2.1.2 International Civil Aviation Organization

ICAO is a specialized agency of the United Nations and is the supreme law-making body in international civil aviation.⁵⁹ Within days of the Air India bombing, ICAO convened a special Ad Hoc Committee of Experts, consisting mainly of government representatives from around the world, to discuss security weaknesses that had led to the bombing.⁶⁰ Key issues included the baggage that CP Air had accepted for interlining without a reservation on the onward flight, and the handling of the interlined baggage that arrived in Toronto without its corresponding passenger.⁶¹ ICAO recognized that the international civil aviation security regime and Annex 17 to the *Convention on International Civil Aviation* (“*Chicago Convention*”) in particular, had been wholly inadequate in dealing with the threat of sabotage. Annex 17, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, governs civil aviation security and outlines the security standards with which all Contracting States must comply. On July 10, 1985, the ICAO Council requested a complete review of Annex 17. A wholesale revision of the Annex followed, among the most significant in its history. The Ad Hoc Committee made recommendations that led to fundamental changes in baggage security procedures. However, one of the most important changes – the introduction of passenger-baggage reconciliation as an international standard – was criticized as inadequate.⁶²

The Ad Hoc Committee had intended to develop a standard for Annex 17 to ensure that no bag would travel if its owner intentionally separated him- or herself from it. This would ensure that no extraneous bag would infiltrate the airline system, as had occurred with Air India. The matching of passengers on board with baggage to be loaded was seen as the primary countermeasure.⁶³ Both IATA and Transport Canada, through its representative, were strong proponents of a comprehensive measure. Indeed, Canada championed the cause of passenger-baggage reconciliation on the international stage.⁶⁴

⁵⁶ See Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4486, 4495.

⁵⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4477, 4486.

⁵⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477.

⁵⁹ Wallis, *Combating Air Terrorism*, p. 91.

⁶⁰ Wallis, *Lockerbie*, p. 11; see also Wallis, *Combating Air Terrorism*, p. 5.

⁶¹ Wallis, *Combating Air Terrorism*, p. 7.

⁶² Wallis, *Lockerbie*, p. 11.

⁶³ Wallis, *Lockerbie*, p. 11.

⁶⁴ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4755–4756.

Transport Canada pushed for a strict rule where no unaccompanied baggage could travel, regardless of the circumstances. Its position was reflected in the simple maxim, "...no passenger, no bag." IATA did not support this proposal, maintaining that such a measure was unrealistic, since there were many reasons that a bag might need to be carried unaccompanied,⁶⁵ including its mishandling by airlines.⁶⁶ Wallis argued on behalf of IATA that unaccompanied baggage should be permitted on aircraft if subjected to the highest degree of scrutiny.⁶⁷ Thoroughly screened baggage, he stated, should not be considered dangerous. ICAO accepted this position.⁶⁸

The text that was eventually published in Annex 17 as Standard 5.1.4 was a compromise. It did not satisfy Canada's or IATA's original intent or that of the Ad Hoc Committee. The text of Standard 5.1.4 read:

Each Contracting State shall establish measures to ensure that operators providing service to or from that State do not place or keep the baggage of passengers who have registered, but have not reported for embarkation, on board the aircraft, without subjecting it to security control.⁶⁹

This rule ensured that all baggage, including interlined baggage,⁷⁰ belonging to booked passengers who did not present for boarding⁷¹ on international flights⁷² would not be loaded onto or transported on an aircraft. However, the unaccompanied baggage that had arrived in Toronto in June 1985 to be transferred to Air India Flight 182 was not associated with a booked passenger because "M. Singh" did not have a reservation on that flight. This situation was therefore not captured by the rule. In other words, infiltration of the airline system by an unaccompanied bag was not covered,⁷³ and the rule, as written, would not have prevented the bombing of Air India Flight 182.⁷⁴

A further problem arose because some states, lobbied by their national airlines, interpreted the rule as allowing unaccompanied baggage to travel if it had been subjected to security controls *before* the discovery of a "no show" passenger. Such security controls would have included X-ray machines and vapour detection equipment, both of which were insufficiently developed to be used as the sole

⁶⁵ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477.

⁶⁶ Wallis, *Lockerbie*, p. 12.

⁶⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477.

⁶⁸ Exhibit P-269, p. 12.

⁶⁹ "Security control" was defined in Annex 17 as "...[a] means by which the introduction of weapons or articles likely to be utilized to commit an act of unlawful interference can be prevented." See Exhibit P-153, pp. 7, 12 of 47.

⁷⁰ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4500.

⁷¹ Such passengers are referred to as "no shows."

⁷² Annex 17 standards and recommended practices apply only to international flights. ICAO does not legislate for domestic services. See Wallis, *Lockerbie*, p. 11.

⁷³ Wallis, *Lockerbie*, p. 11.

⁷⁴ Wallis, *Lockerbie*, p. 11.

security controls.⁷⁵ The security controls described in Standard 5.1.4 were meant to be applied to baggage *after* it had been identified as unaccompanied, not before.⁷⁶

Watered-down provisions are not unusual at ICAO due to the consensus model that has been adopted for their approval.⁷⁷ States with limited financial resources are often unable to agree to stronger, often costlier, provisions. The consequence is an imperfect text that reflects the “lowest common denominator” in security.⁷⁸ Since Annex 17 essentially sets minimum standards, developed countries are always encouraged to exceed the standards.⁷⁹ As will be discussed, the US Federal Aviation Administration (FAA) did just that for passenger-baggage reconciliation. However, insufficient compliance monitoring meant that Pan Am’s discontinuance of reconciliation before the 1988 Lockerbie tragedy went unnoticed.

The ICAO rule respecting passenger-baggage reconciliation applied as of December 19, 1987, but states were encouraged to implement the rule beforehand as soon as was practicable and feasible.⁸⁰ The implementation date was then delayed until April 1989 to enable the technical aspects of automated reconciliation to be resolved.⁸¹ However, those states capable of implementing the procedure sooner were urged to do so.⁸²

As discussed, the addition of this standard was part of a major revision of Annex 17 conducted by the Ad Hoc Committee of Experts. The Committee was later renamed the Panel of Aviation Security Experts⁸³ and eventually came to be known as the AVSEC Panel.⁸⁴ It was given a permanent mandate to investigate acts of unlawful interference with civil aviation and to develop amendments to security measures for worldwide adoption. The Panel was to meet annually to review the security measures in Annex 17 and recommend new provisions. In March 1986, a completely revised and expanded Annex 17 was published,⁸⁵ with 35 mandatory international standards, where previously that had only been 13.⁸⁶ This was the first comprehensive review of Annex 17 since its adoption in 1974,⁸⁷ and remains one of its most fundamental.⁸⁸

⁷⁵ Wallis, *Lockerbie*, p. 12.

⁷⁶ Wallis, *Lockerbie*, p. 11.

⁷⁷ Wallis, *Lockerbie*, p. 11.

⁷⁸ Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4218-4219.

⁷⁹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4218.

⁸⁰ Exhibit P-153, p. (vii); see also Wallis, *Lockerbie*, p. 12.

⁸¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4484.

⁸² Contracting States can withdraw from their obligations under Annex 17 by informing ICAO of their inability or unwillingness to comply. The economic consequences, however, such as loss of air services and insurance coverage, can be substantial: Exhibit P-157, pp. 78-79.

⁸³ Wallis, *Lockerbie*, p. 11.

⁸⁴ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

⁸⁵ Exhibit P-157, p. 88 of 135; see also Wallis, *Lockerbie*, p. 11.

⁸⁶ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

⁸⁷ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

⁸⁸ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4219.

The revision of Annex 17 was necessary to improve counter-sabotage measures in civil aviation security. Still, many security weaknesses revealed by the Air India bombing were not adequately addressed. IATA placed proposals before ICAO to enhance air cargo security, but these did not find sufficient support among Contracting States following the bombing.⁸⁹ The concept of 100 per cent hold bag screening also failed to gain widespread support. It was not until after the bombing of Pan Am Flight 103 and the September 11, 2001, attacks that a more comprehensive approach to address security deficiencies took hold.⁹⁰

Additional ICAO developments included the establishment of a “model clause” on security to be used as part of the basic language governing bilateral air agreements between countries. As well, ICAO began to conduct security surveys at airports that requested assistance, providing recommendations for improvements. More affluent states such as Canada provided assistance in the form of security experts and funding for states in need. In addition, ICAO developed a list of high-risk air carriers and imposed heightened security measures on them.⁹¹

During this period Canada played a significant role at ICAO and in helping to develop several international aviation security initiatives. Canada’s role there continues to be prominent.⁹²

2.1.3 United States: Federal Aviation Administration

Unlike the ICAO standard, the rule implemented by the US Federal Aviation Administration (FAA) to address security gaps exposed by the Air India bombing was comprehensive. The FAA introduced a passenger-baggage reconciliation requirement for US airlines in November 1985, well ahead of the publication of the ICAO standard. The FAA rule required all airlines with flights operating at extraordinary-risk airports to “...conduct a positive passenger/checked baggage match resulting in physical inspection or non carriage of all unaccompanied bags.”⁹³

According to Wallis, this was a foolproof rule. It applied to interlined baggage and, if correctly employed, would prevent an extraneous bag from infiltrating the system. Unfortunately, the FAA failed to monitor its implementation, and was unaware in 1988 that Pan Am had dropped the procedure at both its Frankfurt and London operations. The bombing of Pan Am Flight 103 demonstrated that the development of rigorous rules by regulatory authorities is not sufficient. Their application must be properly monitored as well.⁹⁴

⁸⁹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

⁹⁰ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

⁹¹ Exhibit P-157, p. 88 of 135.

⁹² Exhibit P-157, p. 89 of 135.

⁹³ Wallis, *Lockerbie*, p. 12.

⁹⁴ Wallis, *Combating Air Terrorism*, p. 37.

2.1.4 Ireland: Coroner's Inquest

A coroner's inquest relating to Air India Flight 182 took place in Cork, Ireland, from September 17 to 24, 1985.⁹⁵ The inquest was to establish the identities of the Air India victims and determine how, where and when they died.⁹⁶ Cornelius Riordan, the Cork County Coroner, presided over a jury of ten local citizens. There was a significant Canadian presence as well, including Ivan Whitehall, counsel for Canada's Department of Justice; Robert Hathaway of the Canadian Embassy in Dublin, representing the Government of Canada; and Bruce Garrow, counsel from Canada attending on behalf of a number of the victims' relatives.⁹⁷ The inquest heard testimony from air traffic controllers, navy officers and others who participated in the recovery process, representatives of Air India, pathologists who examined the bodies, and police officers who coordinated emergency services following the crash.⁹⁸

During the inquest, Whitehall argued that a bomb was only one of several possibilities and that there was "no evidence"⁹⁹ to indicate the nature of what had occurred on the aircraft. This conflicted with evidence presented by Dr. Ian Hill, a British aviation pathologist, who concluded that there was a "good chance"¹⁰⁰ that an explosive decompression had occurred, caused either by an explosion or by structural failure. Although Hill found no evidence of an explosive device,¹⁰¹ he believed that the available evidence was consistent with a "catastrophic event"¹⁰² that had occurred at altitude, leading to the breakup of the aircraft in mid-air.¹⁰³

When the coroner requested that certain forensic reports from police laboratories form part of the record at the inquest,¹⁰⁴ the Irish State Solicitor, Barry Galvin,¹⁰⁵ asserted that these reports were being used by the RCMP in its investigation into the possibility of a "criminal act"¹⁰⁶ – a fact that, in itself, might have served to undermine the Canadian position at the inquest. Galvin insisted that the reports were privileged¹⁰⁷ and should not be made public. Although the coroner persisted with his requests, he relented on the final day of the inquest.¹⁰⁸

⁹⁵ See Volume Two: Part 2, Post-Bombing, Section 5.1, Early Government Response for an analysis of Canada's participation at the inquest.

⁹⁶ Public Production 3428, p. 1 of 2 (entered on December 13, 2007 as a compendium of documents on DVD as Exhibit P-391).

⁹⁷ Public Production 3428, p. 1 of 2 (entered on December 13, 2007 as a compendium of documents on DVD as Exhibit P-391).

⁹⁸ Public Production 3428, pp. 1-2 of 2 (entered on December 13, 2007 as a compendium of documents on DVD as Exhibit P-391).

⁹⁹ Exhibit P-101 CAE0339, p. 3 of 4.

¹⁰⁰ Exhibit P-101 CAE0339, p. 2 of 4.

¹⁰¹ Exhibit P-101 CAE0339, p. 2 of 4.

¹⁰² Exhibit P-101 CAE0339, p. 2 of 4.

¹⁰³ Exhibit P-101 CAE0339, p. 2 of 4.

¹⁰⁴ Exhibit P-101 CAE0339, p. 3 of 4.

¹⁰⁵ Public Production 3428, p. 1 of 2 (entered on December 13, 2007 as a compendium of documents on DVD as Exhibit P-391).

¹⁰⁶ Exhibit P-101 CAE0339, p. 3 of 4.

¹⁰⁷ Exhibit P-101 CAE0339, p. 3 of 4.

¹⁰⁸ Exhibit P-101 CAE0339, p. 3 of 4.

At the conclusion of the inquest, Hathaway reported that the coroner “appeared to have made up his mind”¹⁰⁹ that the disaster was most likely caused by a bomb. The coroner considered instructing the jury to recommend closer scrutiny of baggage at airports. Indeed, Garrow argued that deficiencies in airport security had caused baggage to be interlined to Air India without confirmation that the corresponding passengers were on board.¹¹⁰ In response, Whitehall attempted to impose restrictions on the scope of the inquest. He argued that the coroner’s powers were limited by legislation to determining the cause of death and identity of the victims. He maintained that there were a number of possible causes for the crash, that the inquest had not heard all the available evidence, that only medical evidence had been presented and that another investigation with a wider mandate was then in progress.¹¹¹ He submitted that there was no evidence to indicate that security failings at either the Montreal or Toronto airports had caused the crash. This position was taken in spite of a confidential security audit conducted in Canada in July 1985, which revealed significant security failings at both airports. In addition to finding weak airside and aircraft security, the audit noted that there was inadequate protection of checked baggage at Toronto’s Pearson International Airport.¹¹² Yet Whitehall asserted at the inquest that there was “no basis for speculation unsupported by evidence.”¹¹³

In the end, Canada’s position at the inquest prevailed. Hathaway reported that, as a result of the arguments made on behalf of the Government of Canada, the coroner “ultimately accepted”¹¹⁴ Canada’s position and instructed the jury that there was no conclusive evidence as to the cause of the crash and that no recommendations should be made.¹¹⁵

On September 24, 1985, the final day of the inquest, an unprecedented review of airport and airline security in Canada was released. The review had been commissioned by the Government of Canada in response to the events of June 23, 1985.¹¹⁶ This review, known as the Seaborn Report, made recommendations designed expressly to help Canadian aviation security prevent sabotage.¹¹⁷

2.1.5 India: Kirpal Commission

Because the Flight 182 bombing occurred over international waters, the Government of India was designated as the investigative authority in accordance with ICAO Annex 13, which dealt with aircraft accident investigations.¹¹⁸ The Honourable Mr. Justice B.N. Kirpal, Judge of the High Court of Delhi, was

¹⁰⁹ Exhibit P-101 CAE0339, p. 3 of 4.

¹¹⁰ Exhibit P-101 CAF0878, p. 1 of 8.

¹¹¹ Exhibit P-101 CAE0339, p. 3 of 4. Whitehall was likely referring to the work of the Kirpal Commission, discussed below; see also Exhibit P-164.

¹¹² Exhibit P-457, p. 19 of 27.

¹¹³ Exhibit P-101 CAE0339, p. 4 of 4.

¹¹⁴ Exhibit P-101 CAE0339, p. 4 of 4.

¹¹⁵ Exhibit P-101 CAE0339, p. 4 of 4.

¹¹⁶ Exhibit P-101 CAF0039, p. 1 of 10.

¹¹⁷ Exhibit P-101 CAF0039, p. 5 of 10.

¹¹⁸ Exhibit P-164, p. 3.

appointed by the Government of India to lead a formal investigation into the causes and circumstances of the disaster.¹¹⁹ On February 26, 1986, after a lengthy and thorough investigation, the Kirpal Commission presented a report.¹²⁰

The Commission concluded that the detonation of a bomb on board the *Kanishka* was the only plausible explanation for its disappearance:

After going through the entire record we find that there is circumstantial as well as direct evidence which directly points to the cause of the accident as being that of an explosion of a bomb in the forward cargo hold of the aircraft. At the same time there is complete lack of evidence to indicate that there was any structural failure.¹²¹

While much of the report dealt with forensic findings and safety matters, the Kirpal Commission recognized the need to address security issues. The Commission directed its recommendations about aviation security to ICAO, IATA, governments and industry. The recommendations aimed to improve security and prevent explosives from being placed aboard commercial aircraft.¹²² To this end, the report recommended that ICAO, IATA and state governments undertake an ongoing review of established aviation security standards for preventing explosives being placed aboard aircraft. The report called for the creation of a system to monitor security measures implemented in airports around the world, along with a means of reporting findings and suggesting improvements for each airport studied.¹²³ It also recommended that ICAO develop a “model clause” on security, for use in bilateral air agreements, to govern the exchange of mutual air traffic rights, and that ICAO consider establishing training standards for security personnel.¹²⁴ Both ICAO and IATA responded to these recommendations.¹²⁵

The Kirpal Commission made comprehensive recommendations to address the security deficiencies that it had identified as leading to the bombing of Flight 182. Several recommendations pertained to security measures for interlined passengers and their baggage, passenger-baggage reconciliation and unaccompanied baggage:

- IATA should develop practical procedures for reconciliation of interlined passengers and their baggage at intermediate airports;
- Interlining of checked baggage should not occur without a confirmed reservation on the onward carrier flight;

¹¹⁹ See Volume Two: Part 2, Post-Bombing, Section 5.1, Early Government Response for an analysis of Canada’s participation at the Kirpal Commission.

¹²⁰ Exhibit P-164, p. 172.

¹²¹ Exhibit P-164, pp. 159-160.

¹²² Exhibit P-157, p. 78 of 135.

¹²³ Exhibit P-164, p. 172, Recommendation 5.1(a) and (b).

¹²⁴ Exhibit P-164, p. 172, Recommendation 5.2(a) and (b).

¹²⁵ Exhibit P-157, pp. 88-89 of 135.

- The baggage of interlined passengers should be matched with passengers by the onward carrier before being loaded onto the aircraft;
- A passenger count should be done at the boarding gate and, in the case of a passenger “No Show,” the passenger’s baggage must be offloaded;
- All checked baggage, regardless of whether it has been screened by X-ray machine or not, should be personally matched and identified with the passengers boarding an aircraft, and any baggage not so identified should be offloaded; and
- All unaccompanied bags should be placed aboard the aircraft only after their contents have been physically checked, or alternatively, after being placed in a decompression chamber and where the host state is satisfied that the baggage is clean and the shipper has been identified.¹²⁶

The Kirpal Commission also made recommendations relating to intelligence communication during times of “high security threats”:

- Whenever a government becomes aware of a particular high risk security threat, it should notify not only the airline at risk, but also all connecting airlines to ensure that extra precaution can be taken at potential points of introduction of interline baggage into the system; and
- When an airline is aware of a high security threat, it should inform the host state, and if possible and prudent to do so, other airlines operating there.¹²⁷

The Kirpal Commission warned against excessive reliance on technology. It commented on the known failings of the available screening equipment. Significantly, it recommended offloading checked baggage that had not been matched with passengers, even if it had been subjected to X-ray screening. The Commission explained:

...[E]xamination of the baggage with the help of an X-ray machine has its own limitations and is not foolproof. Some explosives hidden in Radios, Cameras, etc. may not be readily detected by such a machine. In fact an explosive not placed in a metallic container will not be detectable by an X-ray machine. Similarly, a plastic explosive can be given an innocuous shape or form so as to avoid detection by an X-ray. Reliance on an X-ray machine alone may in fact provide a false sense of security.¹²⁸

¹²⁶ Exhibit P-164, pp. 172, Recommendations 5.3, 5.4, 5.5, 5.8, 5.9, 5.11.

¹²⁷ Exhibit P-164, pp. 172-174.

¹²⁸ Exhibit P-164, p. 173, Recommendation 5.9.

In a separate recommendation, the Kirpal Commission singled out the inadequacy of the PD-4 “sniffer” upon which Air India had placed sole reliance for screening checked baggage on June 22, 1985, when the X-ray machine in Toronto broke down: “...Effectiveness of the instrument known as PD-4 is highly questionable. It is not advisable to rely on it.”¹²⁹

The Commission recommended that airlines ensure that they have effective backup equipment or procedures in the event of a breakdown of security equipment.¹³⁰

Many of the Kirpal recommendations, including passenger-baggage reconciliation, were eventually adopted worldwide,¹³¹ and numerous other recommendations were implemented by Canada.¹³²

2.2 Canadian Response

2.2.1 Introduction

The Canadian response to the Air India bombing was swift. On June 23, 1985, the day of the bombing, Transport Canada introduced additional security measures for all international flights leaving Canada. These measures were implemented by directing Canadian and foreign air carriers to amend their security programs, rather than by adopting new regulations.¹³³ The measures included:

- More rigorous screening of passengers and their carry-on baggage;
- The physical or X-ray inspection of all checked baggage (this measure was later extended to domestic flights);¹³⁴
- A 24-hour hold on cargo, except perishables from known shippers, unless a physical search or X-ray inspection had occurred;
- The acquisition and deployment of 26 new explosives detector units (then in the final stages of development and testing); and
- The acquisition and deployment of additional X-ray units for carry-on baggage, hand-held metal detectors and walk-through metal-detector units.¹³⁵

All checked baggage interlined to Air India flights was also to undergo physical or X-ray inspection.¹³⁶ It does not appear that this requirement was extended to baggage interlined to other air carriers.

¹²⁹ Exhibit P-436, p. 30; Exhibit P-164, p. 173, Recommendation 5.10.

¹³⁰ Exhibit P-164, p. 174, Recommendation 5.12.

¹³¹ Exhibit P-157, p. 78 of 135.

¹³² Exhibit P-35, p. 20.

¹³³ Exhibit P-157, p. 79 of 135.

¹³⁴ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4485.

¹³⁵ Exhibit P-35, p. 19.

¹³⁶ Exhibit P-263, Tab 14, p. 1 of 6.

When Transport Canada introduced these additional security requirements, air carriers were initially required to conduct hand searches of all checked baggage to be carried on international flights. This caused delays, and Transport Canada recognized that the practice was not sustainable in the long term.¹³⁷ Over the months that followed, the application of the Transport Canada measures was clarified.¹³⁸ Additional Linescan II X-ray machines, with wider apertures, were deployed to ensure that a combination of hand searching and X-ray scanning of checked baggage was in place until passenger-baggage reconciliation could be implemented.¹³⁹

These measures recognized the need for enhanced security in the immediate aftermath of the bombing, but they did not sufficiently address the problem of bombs placed in unaccompanied baggage. When asked whether these measures could have prevented the bombing, Jean Barrette, Director of Security Operations at Transport Canada at the time of the Commission hearings, responded "...No, obviously the reconciliation of passenger baggage...was key."¹⁴⁰

Although Canada was instrumental at the international level in the days following the bombing, steadfastly promoting mandatory passenger-baggage reconciliation, it did not immediately implement the procedure itself.¹⁴¹ Passenger-baggage reconciliation had been used successfully in Canada by KLM and CP Air in the context of a bomb threat in 1984.¹⁴² Reconciliation should have been implemented by Air India in June 1985 because of the elevated threat facing the airline.

The Commission heard evidence that it was not possible for all airlines to implement this measure immediately following the Air India bombing.¹⁴³ The simplest form of reconciliation would have been the identification of baggage by passengers before they boarded, as done in 1984. While this was feasible at smaller airports, major airports required some form of automation.¹⁴⁴ Manufacturers could not immediately provide the appropriate technology, an inability reflected in the delayed implementation of Standard 5.1.4 of ICAO's Annex 17.¹⁴⁵ Nevertheless, Canada was the first ICAO member country to require passenger-baggage reconciliation on international flights before the publication of the ICAO standard. Canada later extended the measure to domestic flights.¹⁴⁶

¹³⁷ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4485.

¹³⁸ Exhibit P-263, Tab 14, p. 1 of 6.

¹³⁹ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4485.

¹⁴⁰ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4509.

¹⁴¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477.

¹⁴² Exhibit P-101 CAF0637, pp. 18-19.

¹⁴³ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4478-4479.

¹⁴⁴ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4478.

¹⁴⁵ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4479.

¹⁴⁶ Exhibit P-35, p. 20.

Measures used in place of passenger-baggage reconciliation did not adequately address the threat of bombs in checked baggage, let alone unaccompanied baggage. X-ray machines provided only black and white images¹⁴⁷ and were known to be a largely cosmetic form of security.¹⁴⁸ The Kirpal Commission recognized this,¹⁴⁹ and Wallis testified that, even with skilled operators, the value of X-rays in screening for explosives was limited:

...[X]-rays were not designed as bomb detecting pieces of equipment. They were designed to identify images. If you were successful in hiding an image, then the screener wouldn't pick it up. That's always assuming the screener had been trained to pick up images and was conscientious in his program.¹⁵⁰

This Commission heard evidence that even hand searches required skilled and knowledgeable screeners, and that electronic equipment in baggage, which could conceal explosives, would need thorough inspection.¹⁵¹ It was unlikely that sufficiently skilled screening personnel would be immediately available to handle the sudden influx of X-ray machines for screening checked baggage.

Both Wallis and Dr. Peter St. John, a former professor of international relations with expertise in air terrorism, warned of the danger of implementing security measures too rapidly. St. John warned that confusion could result "...when you do too much too quickly."¹⁵² Wallis testified that, to be effective, emergency plans needed to be worked out in advance:

If you have a set of procedures that are working on a day-to-day basis, you can't suddenly ratchet them up to become two or three times as effective overnight. That doesn't work. That creates chaos because the airport won't have the staff to do this. The airlines won't have the staff. Queues build up. They go outside the terminal building. You've created a new target of opportunity for terrorists....

You have to be flexible but governments and airlines have to work together on this. You can't be flexible by receiving a dictate from government. That is a recipe for disaster. The governments and the airlines must have worked in advance on flexibility so that when the government feels the need to bring

¹⁴⁷ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4509.

¹⁴⁸ Wallis, *Lockerbie*, p. 12.

¹⁴⁹ Exhibit P-164, p. 173, Recommendation 5.9.

¹⁵⁰ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4256.

¹⁵¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4418-4419.

¹⁵² Testimony of Peter St. John, vol. 37, May 31, 2007, p. 4510.

something new in, it can be put in as quickly as possible but without creating the hazards that we've seen....¹⁵³

The danger posed by misplaced reliance on X-ray equipment may have been mitigated somewhat by the deployment of explosive vapour detection (EVD) units across Canada immediately after the Air India bombing. Designed for screening hold baggage, the units had been under development since the 1970s.¹⁵⁴ In the aftermath of the bombing, Transport Canada expedited the installation of 26 units at major Canadian airports. This equipment was known to be effective in explosives detection and became increasingly sophisticated and reliable in the years to follow.¹⁵⁵ As early as the late 1980s, the Canadian-developed EVD technology became the world standard.¹⁵⁶

In addition to reconciliation procedures, Transport Canada reported in a briefing to the Hon. Bob Rae that it had already acted on several recommendations from the Kirpal Commission. These included: continuous monitoring by trained security inspectors at airports; participation in ICAO's AVSEC Panel; participation in international technical groups, including those involving explosives-detection technologies; continuous assessment of world events that could affect international and domestic aviation security; and assessment and dissemination of information received from intelligence agencies worldwide.¹⁵⁷ Transport Canada continued to improve its security regime in the late 1980s and 1990s by implementing further Kirpal Commission recommendations. In 1989, Canada adopted a new "model clause" on security as part of its basic language governing bilateral air agreements. Transport Canada also required that any contractual changes between private security companies and air carriers not adversely affect screening standards or performance.¹⁵⁸ Further improvements to Canada's aviation security regime included:

- Consolidating security functions in Transport Canada through the creation of a dedicated, multi-modal, multi-functional group, now known as the Security and Emergency Preparedness Directorate;
- Increasing the complement of security inspectors and personnel dedicated to the Directorate;
- Funding (\$5 million) for the development of new technologies;
- Performing a general overhaul of the regulatory framework, including the creation of a four-level alert system, with security measures adjusted accordingly; and
- Increased and more efficient sharing of security intelligence information with domestic and international partners.¹⁵⁹

¹⁵³ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4508.

¹⁵⁴ Testimony of Jean Barrette, vol. 38, June 1, 2007, pp. 4563-4564.

¹⁵⁵ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4529.

¹⁵⁶ Testimony of Jean Barrette, vol. 38, June 1, 2007, pp. 4563-4564.

¹⁵⁷ Exhibit P-263, Tab 13, p. 2 of 4.

¹⁵⁸ Exhibit P-263, Tab 13, pp. 3-4 of 4.

¹⁵⁹ Exhibit P-263, Tab 13, p. 3 of 4.

Alongside the Kirpal Commission's investigation in India, three important studies were undertaken in Canada to address the destruction of Air India Flight 182 and aviation security:

- A 1985 security audit of the international airports in Toronto, Montreal and Vancouver, conducted in the weeks after the bombing. It revealed significant deficiencies in several areas, including access to restricted and airside areas of airports, and the security of air cargo, mail and the aircraft themselves. It also identified a need for improved monitoring of security procedures and better trained security personnel;
- A Canadian Aviation Safety Board (CASB) study; its report, released in January 1986, was written to assist the Kirpal Commission; and
- An additional study commissioned by the Government of Canada to make a more holistic assessment of aviation security, since the CASB's mandate was limited to the disaster itself.¹⁶⁰ This resulted in a far-reaching and widely-praised report, known as the Seaborn Report, released in September 1985. Foremost among its recommendations, consistent with Canada's position at the meeting of ICAO's Ad Hoc Committee of Experts in the days following the tragedies and with the Kirpal Commission's later recommendations, was that checked baggage not be carried on international flights unless the corresponding passenger was also on board.¹⁶¹

Although the CASB, Kirpal and Seaborn investigations influenced Canada's aviation security program,¹⁶² many of the weaknesses they exposed remain.¹⁶³

2.2.2 1985 Airport Security Audit

On July 4, 1985, the Deputy Minister of Transport requested an audit¹⁶⁴ of Pearson, Mirabel and Vancouver International airports to assess delivery of the Civil Aviation Security Program (CASP) in place at the time and to determine whether Transport Canada, the RCMP and air carriers were fulfilling their responsibilities.¹⁶⁵ The CASP was based on the concept of "...clean aircraft, clean

¹⁶⁰ Exhibit P-35, p. 20.

¹⁶¹ Exhibit P-35, p. 20.

¹⁶² Exhibit P-157, p. 75 of 135.

¹⁶³ See Section 3.8, which discusses the current gaps in civil aviation security in Canada.

¹⁶⁴ The audit report contains an introductory note: "Report prepared for Department of Justice Counsel Assessing the Potential for Litigation." Indeed, throughout this Commission's proceedings and after the close of hearings, the Attorney General of Canada exerted a claim of solicitor-client privilege over this document and did not permit its disclosure or use by the Commission, despite protracted negotiations with the Commission. It was not until February 2009 that the Attorney General agreed to release the audit report in full. Although the document was subsequently disclosed to the parties, the result of the delay meant that its full content was not available for examination by all parties during the course of the public hearings: Exhibit P-457.

¹⁶⁵ Exhibit P-457, p. 3 of 27.

passengers, clean baggage, clean cargo and clean mail.”¹⁶⁶ The Internal Audit Branch of Transport Canada conducted the audit and reported its findings on July 25, 1985.¹⁶⁷ The audit focused on four main areas: the screening of passengers, flight crew, baggage, mail, aircraft and cargo; the patrolling of airside areas; the security pass system; and the provision of physical security facilities and equipment.¹⁶⁸ The audit revealed significant deficiencies in each of these areas. Contrary to the CASP directive,¹⁶⁹ the audit was unable to determine the adequacy of air carrier screening of cargo, mail and aircraft, because there were no applicable standards or regulations.¹⁷⁰ The audit report concluded that “... only part of aircraft loads can be considered to be clean in terms of the CASP,”¹⁷¹ because cargo, mail and flight crew baggage were not screened.¹⁷² This is also one of the major findings of the present Commission.

The audit reported such weaknesses as unauthorized access to restricted areas, including cargo and mail warehouses and airside portions of airport terminals. The audit also found deficiencies in the monitoring of security standards, problems with airport and air carrier security plans, weaknesses in addressing different levels of security and inadequate training of security personnel.¹⁷³ Problems with access control included unlocked gates, insecure doors, non-standard fencing, unprotected aircraft and insufficient control and inspection of identification passes.¹⁷⁴ The audit noted that several thousand identification passes could not be accounted for because they had been lost or stolen or not returned by the recipients.¹⁷⁵ In some instances, access doors could be opened with credit cards, or entry codes were written on the doors themselves.¹⁷⁶ “Sterile” areas were sometimes compromised because unscreened passengers from feeder airports were allowed to enter them.¹⁷⁷

The audit found deficiencies in the daily monitoring of security measures and inspection procedures and in follow-up action related to security reviews.¹⁷⁸ Some airport security plans were outdated, and emergency/disaster plans did not define stakeholder responsibilities at different levels of threat.¹⁷⁹ At Pearson International Airport in particular, checked baggage security was inadequate. Control over baggage tags was inconsistent and control over access to accepted baggage awaiting loading was weak.¹⁸⁰ Security personnel were generally insufficiently trained.¹⁸¹

¹⁶⁶ Exhibit P-457, p. 6 of 27.

¹⁶⁷ Exhibit P-457, p. 1 of 27.

¹⁶⁸ Exhibit P-457, p. 5. of 27.

¹⁶⁹ Exhibit P-457, p. 10 of 27.

¹⁷⁰ Exhibit P-457, p. 6 of 27.

¹⁷¹ Exhibit P-457, p. 24 of 27.

¹⁷² Exhibit P-169, p. 52 of 202.

¹⁷³ Exhibit P-101 CAF0695, p. 1 of 3.

¹⁷⁴ Exhibit P-101 CAF0695, p. 1 of 3.

¹⁷⁵ This was noted at Toronto's Pearson International Airport: Exhibit P-457, p. 13 of 27.

¹⁷⁶ Exhibit P-457, p. 14 of 27.

¹⁷⁷ This was specifically noted at Toronto's Pearson International Airport: Exhibit P-457, p. 18 of 27.

¹⁷⁸ Exhibit P-101 CAF0695, p. 2 of 3.

¹⁷⁹ Exhibit P-457, p. 13 of 27.

¹⁸⁰ Exhibit P-457, p. 19 of 27.

¹⁸¹ Exhibit P-457, pp. 17-18 of 27.

A post-audit Transport Canada memorandum addressed to the Deputy Minister proposed a plan to address the major deficiencies. Both short- and long-term initiatives were included:

- Development of new cargo and mail screening requirements;¹⁸²
- Facility improvements and repairs;
- Increased monitoring of access points by security personnel and airlines;
- New regulations to enhance enforcement of access control through sanctions and fines;
- Increased regulatory inspections and spot checks of access points;
- Strengthened standards, guidelines and follow-up procedures for day-to-day monitoring of security measures, including air cargo security;
- Updated airport and air carrier security plans and implementation of test exercises;
- Development of staffing requirements for different threat levels; and
- Establishment of a security awareness program for airport workers and users.¹⁸³

The deficiencies were to be corrected on a high-priority basis,¹⁸⁴ but many remain today. In particular, air cargo and mail, as well as restricted and airside areas of airports, remain vulnerable.¹⁸⁵ In addition, stakeholder security plans, training of security personnel and security awareness have been singled out as still needing improvement.

2.2.3 Seaborn Report

Because of the Air India bombing, the Government of Canada requested the Interdepartmental Committee on Security and Intelligence to undertake an overall review of airport and airline security in Canada, under Intelligence and Security Coordinator Blair Seaborn.¹⁸⁶ When it was released on September 24, 1985, the Seaborn Report was widely praised at home and abroad as a seminal document in civil aviation security. Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the Commission hearings, spoke of the report's importance:

¹⁸² Exhibit P-101 CAF0555, p. 9 of 10.

¹⁸³ See, generally, Exhibit P-101 CAF0695.

¹⁸⁴ Exhibit P-101 CAF0695, p. 3 of 3.

¹⁸⁵ See Sections 3.8.1 and 3.8.2, which discuss the deficiencies in air cargo and airport security, respectively.

¹⁸⁶ Exhibit P-101 CAF0039, p. 1.

The Seaborn Report really became a strategic plan for the Department for many years to follow. It outlined a large number of practices...to further enhance aviation security. And the Department very aggressively pursued implementation of all recommendations in the Seaborn Report over the course of the coming years, in conjunction with and in coordination with other federal government departments that had security responsibilities, and, of course, in conjunction and in coordination with the aviation industry, airlines, airports and labour groups with airports and airlines for that matter.

So it was really a roadmap to take aviation security in Canada from where it was in the aftermath of 1985 to a new and much higher ground. I think it's also important to recognize that not only was it a significant report for Canadian aviation security but also for international aviation security.

...[T]he recommendations implemented by Canada became standards...or benchmarks against which international aviation security evolved and looked to.¹⁸⁷

Indeed, the report highlighted several general principles that remain relevant today. It cautioned that terrorism should not be permitted to interfere unduly with the activities of daily life, but recognized the vulnerability of air travellers to terrorist attacks.¹⁸⁸ It advised that the needs of security must be balanced with the need to facilitate travel.¹⁸⁹ The report emphasized the importance of sharing and integrating security information, integrating decision-making and establishing clear lines of authority.¹⁹⁰ It called for greater security awareness, a proactive approach,¹⁹¹ effective coordination among stakeholders in aviation security¹⁹² and practical means for improving security. The report recommended a graduated system of security measures, to be adjusted according to the level of threat,¹⁹³ with rigorous procedures established even for normal threat levels.¹⁹⁴ During the work of the Commission, many experts and stakeholders stressed similar measures as components of strong aviation security.

The Seaborn Report identified checked baggage and air cargo as particularly vulnerable to sabotage. It outlined screening measures for both, with adjustments made according to levels of threat: normal, enhanced and high.¹⁹⁵ As discussed, one of the most significant changes resulting from the Seaborn Report was

¹⁸⁷ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4504-4505.

¹⁸⁸ Exhibit P-101 CAF0039, p. 7.

¹⁸⁹ Exhibit P-101 CAF0039, p. 1.

¹⁹⁰ Exhibit P-157, p. 75 of 135.

¹⁹¹ Exhibit P-101 CAF0039, p. 1.

¹⁹² Exhibit P-101 CAF0039, p. 3.

¹⁹³ Exhibit P-101 CAF0039, p. 9.

¹⁹⁴ Exhibit P-101 CAF0039, p. 4.

¹⁹⁵ Exhibit P-101 CAF0039, pp. 3-4.

passenger-baggage reconciliation, which Seaborn considered a “better front-line defence against sabotage” than X-raying checked baggage during normal threat levels.¹⁹⁶ Instead, the report recommended supplementing reconciliation with a checked baggage “profile” that airline check-in personnel would apply. Additional measures, including X-ray inspection, explosives detection dogs, hand searching of checked baggage and hijacker “profiles,” were suggested for enhanced and high levels of threat.¹⁹⁷

The report noted that terrorists could use small cargo parcels to target specific aircraft, and suggested that these be X-rayed even in normal threat situations.¹⁹⁸ The report recommended subjecting larger cargo to various methods of inspection or to a hold period, as appropriate, during enhanced threat level situations. It stated that new technology for detecting explosives vapour would likely be available within two to three years, and encouraged the continued development of technology for enhancing aviation security, as well as the use of explosives detection dogs.¹⁹⁹ For high threat levels, the report advocated either a ban on cargo or refusal of all cargo that could not be thoroughly inspected.²⁰⁰ For both baggage and air cargo, no exceptions to the rules were to be tolerated when threat levels were enhanced or high.²⁰¹

In 2009, air cargo remains largely unscreened and technology for this purpose is still being developed.

The Seaborn Report did not recommend removing responsibility for screening passengers and baggage from air carriers.²⁰² Instead, it recommended adequate training for those performing screening.²⁰³ The CATSA Act Advisory Review Panel (CATSA Advisory Panel) was asked in November 2005 to review the civil aviation security breaches associated with the Air India bombing. It produced a report, *Air India Flight 182: Aviation Security Issues*, in 2007. The report characterized the screening of passengers and baggage by air carriers as a “serious weakness” that was rectified only after the attacks of September 11th and the creation of CATSA.²⁰⁴

The 2007 CATSA Advisory Panel report also identified shortcomings in airport security. It recommended full screening of passengers and materials arriving at international airports from less secure airfields. In addition, it recommended, as a condition of employment, security and criminal background checks for all airside employees and for others with access to sensitive areas of the airport

¹⁹⁶ Exhibit P-157, p. 76 of 135.

¹⁹⁷ Exhibit P-101 CAF0039, p. 4.

¹⁹⁸ Exhibit P-101 CAF0039, p. 4.

¹⁹⁹ Exhibit P-101 CAF0039, p. 4.

²⁰⁰ Exhibit P-101 CAF0039, p. 4.

²⁰¹ Exhibit P-101 CAF0039, p. 5.

²⁰² Exhibit P-157, p. 76 of 135.

²⁰³ Exhibit P-101 CAF0039, p. 5.

²⁰⁴ Exhibit P-157, p. 67 of 135.

or to aircraft.²⁰⁵ The report advised airport management and air carriers to maintain a high level of security awareness throughout the airport and on the airfield. It noted that the public could contribute to enhancing security.²⁰⁶ It described vigilance as key to effective security, meaning careful auditing and regular testing of the system.²⁰⁷

Intelligence was not viewed as reliable for predicting and thwarting specific acts of terrorism. Rather, the main value of intelligence was its usefulness in determining the level of security required for the perceived threat.²⁰⁸ Thus, the report recommended a graduated, multi-level system of security, with appropriate measures at each level.²⁰⁹

In terms of oversight and auditing, the report recommended that the Department of Transport, in consultation with the Solicitor General, report annually to the Prime Minister on the adequacy and effectiveness of the security regulations in place. It also called for reporting about the existence of an up-to-date “war-book” at each airport for managing terrorist incidents.²¹⁰

Many of the Seaborn Report’s recommendations required major changes to Canada’s aviation security regime. Some recommendations were immediately followed. However, it was recognized that others would need to be implemented over the coming years.²¹¹ Of the Seaborn Report’s 15 principal recommendations, 10 were directed towards Transport Canada and procedures for strengthening aviation security. The CATSA Advisory Panel observed that all 15 were accepted in principle and eventually addressed to some degree.²¹² As a result of the Seaborn Report, Canada was the first ICAO member to require passenger-baggage reconciliation on international (and, later, domestic) flights, comprehensive background checks for airport workers, removal of coin-operated baggage lockers from major airports and bans on the use of cameras around security checkpoints.²¹³

The Seaborn Report had advocated a more prescriptive (as opposed to performance-based) regulatory framework because of the magnitude of the systemic failures involved in the Air India tragedy. The CATSA Advisory Panel noted that, given the threat and lack of preparedness, this was an appropriate response at the time. However, the Panel viewed the prescriptive legacy of the Seaborn Report as leading to an overly-detailed, rigid security regime that does not allow for the flexibility required in today’s dynamic threat environment.²¹⁴

205 Exhibit P-101 CAF0039, pp. 5-6.

206 Exhibit P-101 CAF0039, p. 6.

207 Exhibit P-101 CAF0039, p. 7.

208 Exhibit P-101 CAF0039, p. 2.

209 Exhibit P-101 CAF0039, p. 9.

210 Exhibit P-101 CAF0039, p. 7.

211 Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4506-4507.

212 Exhibit P-157, p. 75 of 135.

213 Exhibit P-263, Tab 13, p. 3 of 4.

214 Exhibit P-157, p. 75 of 135.

The Seaborn Report also addressed Canada's performance in civil aviation security. It acknowledged that, before June 23, 1985, the emphasis in aviation security had been on anti-hijacking measures. It concluded that airport and airline security in Canada had "...by and large been adequate and in line with international standards."²¹⁵ This finding is not surprising, not only because ICAO's Annex 17 sets only minimum standards, which developed countries are expected to exceed,²¹⁶ but also because Annex 17 was itself inadequate at the time of the Air India bombing.²¹⁷ The report noted that Transport Canada had responded quickly to the events of June 23, 1985, initiating several comprehensive security measures on all international flights leaving Canada. The report found that the Government was instituting measures to address shortcomings identified by the 1985 security audit of three major airports.²¹⁸

The Seaborn Report included a statement that, at the time of its completion, there was no intelligence to corroborate the theory that a bomb had destroyed Air India Flight 182.²¹⁹ Nevertheless, its focus was on combatting sabotage against civil aviation.²²⁰

There is no doubt that the Seaborn Report played a pivotal role in enhancing aviation security in Canada.²²¹ However, the CATSA Advisory Panel noted the striking similarities between its own recommendations and those of the Seaborn Report more than two decades earlier.²²² Despite the broad recommendations of the Seaborn Report, subsequent improvements to Canada's security regime focused primarily on passenger and baggage security. Few improvements were made to the security of air cargo and mail, and those directed at airport security were not sufficient. Consequently, aviation remains vulnerable to attack.²²³

2.2.4 Canadian Aviation Safety Board Investigation

The Canadian Aviation Safety Board (CASB) completed its investigation of the Air India tragedy on January 22, 1986.²²⁴ This investigation was undertaken to assist the Kirpal Commission in India. Its objective was to identify safety deficiencies and to recommend corrective measures to regulatory and enforcement authorities.²²⁵ Much of the report dealt with the forensic evidence related to the aircraft wreckage and the possible safety and structural causes of the disaster. The CASB report concluded:

²¹⁵ Exhibit P-101 CAF0039, p. 7.

²¹⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4218.

²¹⁷ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

²¹⁸ Exhibit P-101 CAF0039, p. 3.

²¹⁹ Exhibit P-101 CAF0039, p. 2.

²²⁰ Exhibit P-101 CAF0039, p. 1.

²²¹ Exhibit P-157, p. 75 of 135.

²²² See Exhibit P-157, pp. 118, 120 of 135.

²²³ Exhibit P-157, p. 91 of 135.

²²⁴ See Volume Two: Part 2, Post-Bombing, Section 5.1, Early Government Response for an analysis of Canada's subsequent use of the CASB Report at the Kirpal Commission.

²²⁵ Exhibit P-167, Title page.

There is considerable circumstantial and other evidence to indicate that the initial event was an explosion occurring in the forward cargo compartment. This evidence is not conclusive. However, the evidence does not support any other conclusion.²²⁶

Like Seaborn, the CASB report found that the Canadian aviation security arrangements then in place met or exceeded international standards. Also like the Seaborn Report, it emphasized that the focus had been placed on preventing the boarding of weapons, including explosive devices, in hand baggage, and that the screening of checked baggage was undertaken only in circumstances of heightened threat.²²⁷

The CASB report made several findings of fact about the security circumstances of the events of June 22 and 23, 1985. It concluded that the security numbering system used in Toronto did not prevent the unaccompanied interlined baggage from being loaded onto the flight, and that the effectiveness of the explosives detector used by Air India was in doubt.²²⁸ The report found that, had passenger-baggage reconciliation been performed in Toronto, the unaccompanied baggage “would have been detected” and “...airline procedures would have prevented the placement of the suitcase on the aircraft.”²²⁹

2.2.5 Changes to Legislative and Regulatory Framework

Concluding a multi-year effort, the *Aeronautics Act* was amended on June 28, 1985 – just days after the Air India bombing. These amendments were not directly related to the bombing. Most related to safety and enforcement, and some referred to security.²³⁰ The amendments laid the foundation for what was to become Canada’s modern aviation security and enforcement regime.²³¹

The security amendments to the *Aeronautics Act* gave the Minister of Transport greater regulation-making authority over airport operators and persons carrying on activities at airports. The CATSA Advisory Panel explained this authority:

Authority to make regulations applying to Canadian and foreign aircraft was no longer limited to screening activities, but could extend to a wide variety of other security activities required to protect passengers, crew members, aircraft and other aviation facilities. The new rules were expressed in the *Air Carrier Security Regulations* and the *Aerodrome Security Regulations*. The amendments also permitted the Minister of

226 Exhibit P-167, p. 58.

227 Exhibit P-167, p. 54.

228 Exhibit P-167, p. 59.

229 Exhibit P-167, pp. 56-57.

230 Exhibit P-157, p. 79 of 135.

231 Exhibit P-263, Tab 15, p. 1 of 5.

Transport to make confidential orders, called “measures,” to deal with such security-sensitive issues as security of persons and their carry-on baggage and cargo, as well as security screening equipment.²³²

Unauthorized disclosure of these confidential security measures was an offence.²³³

In December 1985, amendments were made to the *Civil Aviation Security Measures Regulations* and its corresponding *Order* and to the *Foreign Aircraft Security Measures Regulations* and *Order*. These amendments authorized the Minister to approve security procedures for a broad range of security purposes and required air carriers to carry them out. In February 1986, Transport Canada issued the first edition of approved security procedures applicable to foreign and domestic air carriers. They prescribed the flights that required screening and detailed the screening procedures required. They also addressed the security of passengers, carry-on baggage, checked baggage and cargo, and included measures applicable to security equipment and security officers. All screening equipment used by air carriers required the Minister’s approval.²³⁴ Passenger-baggage reconciliation counts were required for checked baggage, and the baggage was to be removed if the passenger was not on board.²³⁵

In 1987, the *Air Carrier Security Regulations* replaced the *Civil Aviation Security Measures Regulations* and *Foreign Aircraft Security Measures Regulations* and the corresponding *Orders* associated with each regulation. New *Aerodrome Security Regulations* were introduced at the same time. The *Air Carrier Security Regulations* and *Aerodrome Security Regulations* authorized the Minister to approve air carrier security procedures during periods of normal and increased levels of threat. They required air carriers and airport operators to submit written security programs containing the approved procedures and formalized many internal policies and procedures adopted by Transport Canada as owner and operator of the international and major domestic airports in Canada.²³⁶

The first set of approved security measures for aerodromes was issued in 1987.²³⁷ It dealt with implementing background checks for employees with regular access to restricted areas and flowed from the recommendations of the Seaborn Report. The Aerodrome Restricted Area Access Clearance Program (ARAACP) instituted checks of criminal backgrounds and criminal associations, in addition to the credit checks conducted by Transport Canada.²³⁸

A 1990 Federal Court decision struck down the ARAACP. Transport Canada then corrected what was essentially a legal and drafting problem with the ARAACP

²³² Exhibit P-157, p. 79 of 135.

²³³ Exhibit P-263, Tab 14, p. 1 of 6.

²³⁴ Exhibit P-263, Tab 14, p. 2 of 6.

²³⁵ Exhibit P-157, p. 80 of 135.

²³⁶ Exhibit P-157, p. 80 of 135.

²³⁷ Exhibit P-263, Tab 14, p. 3 of 6.

²³⁸ Exhibit P-157, p. 86 of 135.

by making two new orders – the *Air Carrier Security Measures Order* and the *Aerodrome Security Measures Order*. These orders, by reference, incorporated approved security measures for air carriers and aerodromes, including the ARAACP.²³⁹

2.2.6 Changes in Oversight

2.2.6.1 Roles and Responsibilities

The following roles and responsibilities in Canada's civil aviation security program were prescribed under the June 28, 1985, amendments to the *Aeronautics Act*: The Minister of Transport was responsible for aviation security policy, the regulatory framework and compliance monitoring;

- Airport managers, who were employees of Transport Canada, were responsible for implementing the security measures and procedures prescribed under the *Aerodrome Security Regulations* and the *Aerodrome Security Measures*, including the preparation of security and emergency plans and procedures;
- All commercial air carriers with flights into and out of Canada were responsible for implementing the security measures and procedures prescribed under the *Air Carrier Security Regulations* and the *Air Carrier Security Measures*, and for providing the Minister with an Air Carrier Security Plan; and
- The RCMP was responsible for policing at Canadian international airports and some major domestic airports.²⁴⁰

As the CATSA Advisory Panel observed, the key to any effective security regime is the clear delineation, communication and application of policies and rules by those responsible for their implementation. After the Air India bombing, a Transport Canada task force recommended the establishment of a multi-modal, multi-functional transportation security directorate to oversee security divisions, including intelligence, for all modes of transportation. The Security and Emergency Preparedness Directorate was created in July 1986, and was given responsibility for policy development, the transportation security clearance program and security training guidelines for inspectors and the industry.²⁴¹

2.2.6.2 Inspection and Enforcement

The Transport Canada task force recommended deploying a dedicated team of security inspectors across the country to monitor and inspect airport and air carrier field operations, and to take enforcement action when they saw violations of legislation or regulations. The mandate to monitor, inspect and enforce was

²³⁹ Exhibit P-263, Tab 14, p. 3 of 6.

²⁴⁰ Exhibit P-157, p. 82 of 135.

²⁴¹ Exhibit P-157, pp. 82-83 of 135.

carried out in various ways: inspections of air carriers and airports; monitoring and testing of screening procedures; monitoring and inspection of cargo facilities, air terminal facilities and airside access controls; and certification and designation of security officers. Under the *Aeronautics Act*, inspectors had the authority to inspect, to enter business premises, to search and seize, to detain an aircraft and to levy “administrative monetary penalties” for non-compliance with regulations or measures.²⁴²

Transport Canada undertook a more aggressive and cyclical security inspection program of air carriers and airports, based on threat assessments and consistent with international obligations. By 1990, Transport Canada’s Security Inspection and Compliance Branch included about 30 security inspectors.²⁴³

At the heart of the Department’s aviation security enforcement philosophy was “...the conviction that aerodromes and air carriers would find **voluntary compliance** with regulations and measures to be in their self-interest, as well as in the public interest.”²⁴⁴ Where voluntary compliance was not forthcoming, enforcement action occurred in a manner that attempted to be fair, consistent and uniform across all regions.²⁴⁵ Voluntary compliance was encouraged and supported through education, publicity and the presence of inspectors in the field. The intention of the inspection and enforcement framework was to create conditions where voluntary compliance with regulations was “...the logical, desirable and economically feasible choice for the regulated community.”²⁴⁶ According to Transport Canada, this was a new program designed to provide a wide range of flexible, proactive and proportional options to secure compliance. Inspectors supported the program by carrying out their responsibilities in the four core areas of activity: prevention, detection, investigation and enforcement.²⁴⁷ Seminars and presentations were delivered to individuals, industry groups and outside agencies upon request.²⁴⁸ Publicity programs were designed to increase aviation security awareness and to prevent security violations.²⁴⁹ Providing advice on security matters became an integral component of the day-to-day business of security inspectors.²⁵⁰

²⁴² Exhibit P-157, p. 83 of 135.

²⁴³ Exhibit P-157, p. 83 of 135.

²⁴⁴ Exhibit P-263, Tab 15, p. 3 of 5 [Emphasis in original].

²⁴⁵ Fairness in the enforcement context meant that: the Department’s inspection and enforcement manual were to be made available for public scrutiny to the fullest extent possible, without compromising national security; industry was to be consulted on an ongoing basis, with senior departmental officials accessible to explain the program and receive suggestions for improvement; inspectors were not to exceed their delegated authority in carrying out their duties and were required to declare any apparent or actual conflicts of interest; voluntary compliance was to be encouraged and supported through education, publicity and inspector presence in the field; minor violations were to be handled leniently at first instance, through administrative rather than prosecutorial action; and violations that were pre-meditated or were marked by indifference were to be dealt with vigorously. See Exhibit P-263, Tab 15, pp. 3-4 of 5.

²⁴⁶ Exhibit P-263, Tab 15, p. 4 of 5.

²⁴⁷ Exhibit P-263, Tab 15, p. 4 of 5.

²⁴⁸ Exhibit P-157, p. 84 of 135.

²⁴⁹ Exhibit P-263, Tab 15, p. 4 of 5.

²⁵⁰ Exhibit P-157, p. 84 of 135.

If a security violation occurred, inspectors had a range of enforcement options:

- Emergency action, including detention of aircraft, denial of air traffic control clearance, or emergency suspension of a Canadian aviation document, where circumstances created an immediate threat to aviation security and the public interest;
- Judicial action, by summary conviction prosecution or, upon advice of Crown counsel, by prosecution by indictment; or
- Administrative action, with a series of proportional and graduated responses, beginning with letters of enforcement, proceeding to the imposition of administrative monetary penalties and appearance before a specialized administrative tribunal, and ending with the suspension or cancellation of a Canadian aviation document, or the Minister's refusal to renew.²⁵¹

2.2.7 Changes in Training

Transport Canada created a joint industry-government training task force in response to the Air India bombing. This resulted in improved training programs, certification and inspection standards and testing of passenger screening personnel. Air carriers were responsible for training screening personnel, and Transport Canada was responsible for providing the training materials.²⁵² Transport Canada developed an educational program to ensure a sound knowledge of civil aviation security legislation and the consequences of non-compliance. A training component was designed for pre-board screening personnel, including both practical and written examinations to assess screening officer qualifications.²⁵³ The tests became more difficult, more extensive, and had a higher pass mark. Transport Canada reported that there were a great number of failures initially, and that these individuals were removed from active duty.²⁵⁴

The new training programs were also directed at supervisors and trainers.²⁵⁵ In addition, security training programs were developed for air traffic controllers, flight service station operators, airside employees, passenger agents, pilots and flight crews. Transport Canada provided training and awareness programs for its own airport managers and workers, as it owned and managed most major airports in Canada at the time. In addition, airport security committees met more frequently and provided security updates to airport workers on a regular basis.²⁵⁶ In October 1988, Transport Canada retained three education and training specialists to professionalize the security inspectors' occupational certification program.²⁵⁷

²⁵¹ Exhibit P-263, Tab 15, p. 5 of 5.

²⁵² Exhibit P-157, p. 84 of 135.

²⁵³ Exhibit P-157, p. 84 of 135.

²⁵⁴ Exhibit P-263, Tab 16, p. 1 of 5.

²⁵⁵ Exhibit P-157, p. 84 of 135.

²⁵⁶ Exhibit P-157, p. 85 of 135.

²⁵⁷ Exhibit P-263, Tab 16, p. 1 of 5.

2.2.8 Enhancements in Security Systems and Equipment

By 1985, Transport Canada was already testing explosive vapour detection (EVD) units for hold bag screening, but had not yet deployed them in airports. Immediately after the Air India bombing, the Department expedited the acquisition and installation of 26 units at major airports. Though Transport Canada initially trained its own security officers to operate the EVD units, the RCMP assumed responsibility for training and operating the units in 1987. In 1995, the first series of EVD units were replaced with newer, enhanced units that were portable and that could detect plastic explosives. In 1997, the not-for-profit Air Transport Security Corporation, which was funded by the airlines to deliver screening on their behalf, relieved the RCMP of its responsibility for operating EVD units when it took over the entire screening function on behalf of air carriers.²⁵⁸

Air carriers were responsible for operating and manning the security equipment, which consisted of walk-through and hand-held metal detectors and devices for screening carry-on baggage. Transport Canada initially maintained the equipment. It later transferred its maintenance role to the Air Transport Security Corporation, but before that upgraded the X-ray equipment at 28 major airports from black and white to “dual-energy” colour capable of detecting both explosives and organic material.²⁵⁹

After 1985, additional facilities and systems were established, and equipment purchased, to increase protection of restricted areas and improve passenger and baggage screening. These measures included electronic surveillance systems, key card access control systems, enhanced communication systems, and upgraded fences, security doors and gates. Additional security measures at perimeter access points were also implemented, with upgraded signage and security guards at access gates to collect identifying information from vehicles and their occupants.²⁶⁰

As well, Transport Canada’s research and development program focused on projects to improve aviation security, particularly in those areas exploited by terrorists in the Air India tragedy. Projects included X-ray pattern recognition, enhancement of trace explosives detection equipment, creating walk-through and X-ray explosives detection equipment and automating the passenger-baggage reconciliation process.²⁶¹

2.2.9 Conclusion

The Air India bombing demonstrated the inadequacy of the anti-sabotage measures in place at the time. This led to a transformation of the Canadian and international civil aviation security regimes. Annex 17 to the *Chicago*

²⁵⁸ Exhibit P-157, p. 85 of 135.

²⁵⁹ Exhibit P-157, pp. 85-86 of 135.

²⁶⁰ Exhibit P-157, p. 86 of 135.

²⁶¹ Exhibit P-157, p. 86 of 135.

Convention was completely revised to better address the threat of sabotage, and the Canadian regime was overhauled, with changes to its regulations, an improved system of inspection and enforcement, a clarification of roles and responsibilities, and enhancements to screening technologies. Transport Canada was also instrumental in securing important changes at the international level, in particular the adoption of passenger-baggage reconciliation as an international standard.

The international and domestic responses to the bombing were impressive in many ways, but also sometimes flawed. Although Annex 17 required passenger-baggage reconciliation through the adoption of Standard 5.1.4, this standard was imperfect. The new standard did not address an extraneous bag infiltrating the system – the situation that Air India faced in June 1985. As well, the wording of the Standard was unclear, leading some in the civil aviation community to argue that security controls were not required following the discovery of an unaccompanied bag if some type of screening of the bag for prohibited items had been conducted beforehand.

The immediate emergency response in Canada was also deficient, with continued reliance on X-ray technology that was known to be ineffective for detecting explosives. It would be more than a decade before the technology was adequate for this purpose. The deployment of additional X-ray machines at the time was not an adequate substitute for passenger-baggage reconciliation (admittedly, however, reconciliation was not available for across-the-board application until some months after the bombing). Cosmetic measures might provide a false sense of security and waste precious resources.

The international and Canadian responses were also incomplete. They failed to adequately address other weaknesses revealed by the bombing – specifically, air cargo security and access control at airports. Improved technology to facilitate full hold bag screening was also recognized by many as an important goal. To its credit, the Government of Canada recognized that a limited response was insufficient, and that a holistic review of deficiencies in security was required. In the resulting Seaborn Report, the Government received a guide to comprehensive change, but failed to implement many recommendations.

Support for more systemic improvements was lacking at the international level and there was inadequate follow-through domestically. Enhancements to passenger and baggage security became the primary focus, but even these were not fully addressed. It was only following the bombing of Pan Am Flight 103 (whose method of sabotage paralleled that of the Air India bombing) and September 11, 2001, that more comprehensive, multi-layered solutions to the threat of sabotage began to be implemented.

Because of persistent vulnerabilities in the system following the loss of Air India Flight 182, passenger security continued to be deficient. Bombs could still be introduced by means other than passengers and baggage. More than 20 years later, the 2007 report by the CATSA Advisory Panel noted that many deficiencies

first highlighted in the Seaborn Report remained. While the importance of passenger-baggage reconciliation must not be diminished, the Air India bombing revealed more than just the danger of unaccompanied, infiltrated bags. The bombing exposed other widespread deficiencies in procedures for preventing sabotage. Comprehensive action to improve civil aviation security is long overdue.

2.3 Failure to Learn: The Bombing of Pan Am Flight 103

Had the rules which emanated from the Air India bombing been applied in 1988, Lockerbie would never have happened.²⁶²

The history of civil aviation security shows repeated failures to learn from the past. Some aviation experts, including Rodney Wallis, a former Director of Security at the International Air Transport Association whose words are quoted above, believe that this deafness to what history might teach has seldom been more apparent than in the 1988 bombing of Pan American World Airlines (Pan Am) Flight 103 over Lockerbie, Scotland. The acts that led to the bombing emulated precisely those which led to the destruction of Air India Flight 182 three years earlier. An unaccompanied suitcase concealing a bomb was interlined to Pan Am Flight 103 from a different carrier.²⁶³ Pan Am did not detect the bomb. Yet this method of sabotage was well understood because of the experience gained from the Air India disaster, and international standards had recognized passenger-baggage reconciliation as the incontrovertible solution.²⁶⁴ Still, terrorists launched a successful attack on Flight 103 that killed 270 people.²⁶⁵ The United States Commission on Aviation Security and Terrorism (US Commission), established in August 1989, concluded that the bombing of Flight 103 was preventable:

Stricter baggage reconciliation procedures could have stopped any unaccompanied checked bags from boarding the flight at Frankfurt.²⁶⁶

Like Air India, Pan Am did not use passenger-baggage reconciliation as a security measure. Unlike Air India, Pan Am had been required to do so by US federal regulation – a measure introduced as a direct result of the Air India bombing.²⁶⁷ In testimony before the Commission, Wallis recounted how Pan Am, in a bid to cut costs, unilaterally discarded compulsory passenger-baggage reconciliation. In its place, Pan Am screened interlined baggage for

²⁶² Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4210.

²⁶³ Exhibit P-166, pp. 2-3.

²⁶⁴ Wallis, *Lockerbie*, pp. 11-12.

²⁶⁵ Wallis, *Lockerbie*, p. 1.

²⁶⁶ Wallis, *Lockerbie*, p. 46.

²⁶⁷ Exhibit P-166, p. 3.

explosives using X-ray technology that it knew to be ineffective.²⁶⁸ Air India had made similar decisions in 1985. In both cases, the decision not to implement passenger-baggage reconciliation was symptomatic of broader deficiencies in the security regime. These included insufficient regulatory oversight, a failure of shared responsibility, a misplaced reliance on ineffective technology and an inappropriate balancing of efficiency and security concerns.

The failure to appreciate the lessons of Air India was all the more significant because the Air India disaster was a watershed in the history of aviation security.²⁶⁹ It was the worst aviation terrorism incident the world had seen, and remained so until the events of September 11, 2001.²⁷⁰ The bombing of Flight 182 signalled the urgent need for a shift in focus from preventing hijacking to preventing sabotage,²⁷¹ and was the driving force behind one of the most extensive reforms of the international regulatory regime for civil aviation. The result was a more stringent Annex 17 to the *Convention on International Civil Aviation* ("*Chicago Convention*"), which better addressed the security threats facing civil aviation.²⁷²

The loss of Air India Flight 182 ought to have brought complacency about the threat of sabotage to an end.²⁷³ However, Wallis suggested that it was "a fact of life" to tend to attach more significance to incidents that were seen to affect "the Anglo-Saxon world," rather than people from a different heritage.²⁷⁴ As Peter St. John, a retired professor of international relations with expertise in air terrorism and extensive knowledge of the bombing of Air India Flight 182, observed, "... there was a popular conception in Canada that somehow the Canadians of Indian origin on board Air India 182 were Indian citizens from India, and that it wasn't our crisis and it wasn't our problem."²⁷⁵

2.3.1 Failure to Address the Known Threat of a Bomb in Interlined, Unaccompanied Baggage

Pan Am Flight 103 was a service from Frankfurt to New York, with a transit stop in London. On December 21, 1988, not long after departing London's Heathrow Airport for New York, a bomb detonated aboard the Boeing 747, named *Maid of the Seas*, just as it had reached 31,000 feet above the small town of Lockerbie, Scotland.²⁷⁶ The aircraft shattered and its remains "...rained death and destruction on the town of Lockerbie."²⁷⁷ All 259 passengers and crew on board were killed, along with 11 local residents who died when debris fell to the ground.²⁷⁸

²⁶⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4516-4517.

²⁶⁹ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4288.

²⁷⁰ Exhibit P-35, p. 1.

²⁷¹ Exhibit P-157, p. 75 of 135.

²⁷² Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

²⁷³ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4209.

²⁷⁴ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4527.

²⁷⁵ Testimony of Peter St. John, vol. 37, May 31, 2007, p. 4524.

²⁷⁶ Wallis, *Lockerbie*, p. 1.

²⁷⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4525.

²⁷⁸ Wallis, *Lockerbie*, p. 1.

The *modus operandi* was identical to that used to destroy Air India Flight 182.²⁷⁹ Both Air India and Pan Am had been operating under an elevated level of threat from sabotage.²⁸⁰ As with Air India Flight 182, the bomb that destroyed Pan Am Flight 103 began its journey at an outlying airport from which Pan Am did not operate. The idea was to gain access to the intended aircraft by initially sending the bomb in an interlined, unaccompanied suitcase on the connecting flight of another air carrier – one that was not operating under an elevated level of threat.²⁸¹

The means to attack the *Maid of the Seas* were readily available, and the methodology was a tried and familiar one, proven effective by earlier terrorist groups. In so many ways the loss of the *Maid of the Seas* paralleled the destruction of Air India's *Kanishka* in 1985. In both, an unaccompanied suitcase carrying an improvised explosive device concealed in a cassette radio had been infiltrated into the airline industry's interline baggage system. An airport, off-line to the targeted carrier's route network, had been selected for this purpose. The device was first flown on a feeder service from that airport to another, where it was transferred to the intended aircraft.²⁸²

The similarities between the two incidents warrant a detailed description. In 1985, a passenger appeared at the Canadian Pacific Air (CP Air) ticket counter at Vancouver Airport and checked in a suitcase that contained a bomb. The suitcase was loaded onto a CP Air flight destined for Toronto. At the passenger's insistence, the suitcase was labelled with an interline tag for onward carriage on Air India Flight 181 in Toronto (the flight number changed to 182 during a transit stop in Montreal).²⁸³ An interline tag was placed on the bag in contravention of CP Air's standard security procedures,²⁸⁴ since the passenger did not have a reservation for the subsequent leg of the journey. Once in Toronto, the unaccompanied bag was delivered to the airport's baggage makeup area where it was interlined to the Air India aircraft.²⁸⁵

With Pan Am Flight 103, the bomb was initially placed aboard an Air Malta aircraft in Malta as a result of a breach in airside security. The perpetrator was

²⁷⁹ Exhibit P-166, p. 2.

²⁸⁰ Wallis, *Combating Air Terrorism*, p. 27; see also Exhibit P-157, p. 49 of 135.

²⁸¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4516.

²⁸² Wallis, *Lockerbie*, p. 63.

²⁸³ Exhibit P-436, pp. 18, 20.

²⁸⁴ Exhibit P-436, p. 18.

²⁸⁵ Exhibit P-436, p. 29.

a former chief of security with Libyan Arab Airlines²⁸⁶ whose links to the airline gave him access to the baggage makeup area and, ultimately, to baggage tags. The suitcase concealing the bomb had not gone through normal check-in procedures. It was simply labelled with an interline tag, loaded onto the Air Malta flight and interlined to Pan Am in Frankfurt. Like the situation leading to the bombing of Air India Flight 182, the bag was not accompanied by a corresponding passenger on any segment of its journey.²⁸⁷ Though some of the finer points of the Pan Am and Air India bombings differed, there were many core similarities:

...Introduce your bomb bag at an airport, off-line to the major carrier so that guards are down. The bag slips into the interline system and the interline system carried it onto the target aircraft. So they are identical situations²⁸⁸

By 1988, this *modus operandi* for committing sabotage against aircraft was well known. The loss of Flight 182 in 1985 had sparked an immediate flurry of activity within the international civil aviation community,²⁸⁹ which realized that its security regime had been insufficient against sabotage.²⁹⁰ The result was a complete revision of Annex 17 to the *Chicago Convention*.²⁹¹ The revision established passenger-baggage reconciliation as an international standard.²⁹² Passenger-baggage reconciliation sought to prevent unauthorized bags, possibly containing bombs, from being placed on aircraft by matching checked baggage with passengers on board.²⁹³ Before the bombing of Flight 182, reconciliation procedures had been used on an *ad hoc* basis during periods of high threat,²⁹⁴ but were not a requirement of most aviation security regimes.²⁹⁵ Several international and Canadian reviews of the Air India disaster concluded that passenger-baggage reconciliation was the one measure that, on its own, could have prevented the bombing.²⁹⁶

Although Pan Am and Air India were both operating under an elevated level of threat, neither airline was using passenger-baggage reconciliation around the time of the sabotage against their aircraft. Unlike the situation with Air India in

²⁸⁶ He was also an intelligence officer of the Libyan government. In 2001, he was found guilty of murder in the bombing of Pan Am Flight 103 and was sentenced to 27 years in prison: Wallis, *Combating Air Terrorism*, p. 38.

²⁸⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4516.

²⁸⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4517.

²⁸⁹ Exhibit P-162, pp. 2-3.

²⁹⁰ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

²⁹¹ Annex 17 is the treaty that governs matters of international civil aviation security. See Exhibit P-153, the 1986 revised edition of Annex 17 which resulted from the bombing of Air India Flight 182.

²⁹² Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4217-4218.

²⁹³ Wallis, *Lockerbie*, p. 152.

²⁹⁴ See, for example, Exhibit P-101 CAF0637, pp. 18-19.

²⁹⁵ The Commission received evidence, however, that the United Kingdom's Department of Transport had implemented a rule, prior to 1985, that required bags on flights leaving the country to be reconciled with their passengers.

²⁹⁶ See, for example, Exhibit P-101 CAF0039, p. 4 of 10.

1985, Pan Am was required by law to do passenger-baggage reconciliation for Flight 103.²⁹⁷ Even before the international reconciliation standard took effect, the US Federal Aviation Administration (FAA)²⁹⁸ required reconciliation by all US airlines operating out of airports designated as “extraordinary risk.” Starting in November 1985, the FAA rule required all checked baggage to be matched with passengers on board the aircraft. Any unaccompanied baggage was to be physically inspected or else removed from the flight.²⁹⁹ Rodney Wallis praised the FAA rule, claiming that it should have provided “foolproof protection against the infiltrated, unaccompanied bag.”³⁰⁰ Indeed, in October 1988, before the loss of Flight 103, Dr. Assad Kotaite, then President of the International Civil Aviation Organization (ICAO) Council, hailed reconciliation as “the cornerstone of aviation’s defense against the saboteur.”³⁰¹

The measures implemented after the Air India disaster sought to prevent similar sabotage.³⁰² By late 1988, the FAA had designated all airports in Europe as extraordinary risk.³⁰³ Because of this, Flight 103 was required to conduct passenger-baggage reconciliation.

Both Air India Flight 182 and Pan Am Flight 103 were scheduled to make one transit stop before their transatlantic crossings.³⁰⁴ Flight 103 did more than simply make a transit stop at Heathrow Airport in London. A change of aircraft took place. A Boeing 727 had flown from Frankfurt to London, where a larger jet, a Boeing 747, was waiting to take both Frankfurt- and London-originating passengers on to New York. The two aircraft were parked beside each other, and baggage from the 727 aircraft was placed in a container to be loaded aboard the 747. This presented a further opportunity to do passenger-baggage reconciliation.

Besides the FAA rule, the United Kingdom Department of Transport required all flights leaving the country to reconcile bags with passengers:

This rule had been in place prior to 1985 when the [UK Department of Transport] had emphasized the potential danger arising from interline baggage. In Frankfurt the FAA had mandated U.S. airlines to apply positive passenger/baggage matching procedures; with the same rule applying at Heathrow, the opportunity existed there to identify and

²⁹⁷ Exhibit P-166, p. 3.

²⁹⁸ The Federal Aviation Administration (FAA) is no longer in existence. Since 2001, civil aviation security in the United States is managed by the Transportation Security Administration, which is governed by the Department of Homeland Security (DHS). See Exhibit P-157, p. 96 of 135.

²⁹⁹ Wallis, *Lockerbie*, p. 12.

³⁰⁰ Wallis, *Lockerbie*, p. 46.

³⁰¹ Wallis, *Combating Air Terrorism*, p. 30. Kotaite made this statement in an address to the FAA’s Washington Triennial Aviation Security Conference.

³⁰² Wallis, *Lockerbie*, pp. 1–2.

³⁰³ Wallis, *Combating Air Terrorism*, p. 30.

³⁰⁴ Air India Flight 182 had stopped in Montreal following its departure from Toronto, on its way to London: Exhibit P-436, pp. 37–38.

remove or physically search any unaccompanied bags. Because that did not happen, what should have been a foolproof system was defeated.³⁰⁵

Air India Flight 182 missed one opportunity to match baggage with passengers. Pan Am Flight 103 missed two.³⁰⁶

As mentioned earlier, the US Commission described the bombing of Flight 103 as “preventable.”³⁰⁷ By late 1988, Flight 103 was operating under a heightened level of threat of sabotage, since the FAA had designated all European airports as extraordinary risk for US air carriers. In addition, Pan Am was aware that Flight 103 was a specific target.³⁰⁸ Two months before the bombing, the airline was informed about the discovery of a terrorist ring in Germany that had been manufacturing bombs containing Semtex plastic explosives for detonation on board aircraft. At least two bombs, hidden in Toshiba cassette radios, were known to be in circulation.³⁰⁹ On December 5, 1988, the US Embassy in Helsinki received an anonymous telephone call warning of the bombing of a Pan Am aircraft operating between Frankfurt and the US “within the next two weeks.”³¹⁰ Both Finnish and US authorities concluded at the time that the call was a hoax.³¹¹ Nonetheless, when the warning was received, the FAA shared the details of the threat with Pan Am and other US airlines.³¹²

In summary, according to Wallis, Pan Am management in Frankfurt, in breach of US federal regulations, and despite the elevated threat of sabotage, decided to discontinue its reconciliation practices because of concerns about the cost of matching interlined baggage with passengers.³¹³ In its place, the airline opted to scan interlined baggage for explosives using less expensive X-ray technology.³¹⁴

Pan Am set up a subsidiary company in Frankfurt, Alert Management, to carry out its security operations, and bought new X-ray machines to conduct checked baggage screening. Wallis wrote that the airline concluded that this measure absolved it of the need to match interlined passengers with their baggage.³¹⁵

By 1988, it was well known that X-ray technology was unreliable in detecting explosive devices in checked baggage.³¹⁶ In 1986, the Indian inquiry established to investigate the bombing of Air India Flight 182 (Kirpal Commission) concluded:

³⁰⁵ Wallis, *Combating Air Terrorism*, pp. 26-27.

³⁰⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4517.

³⁰⁷ Wallis, *Lockerbie*, p. 46.

³⁰⁸ Wallis, *Combating Air Terrorism*, p. 27.

³⁰⁹ Wallis, *Combating Air Terrorism*, p. 27.

³¹⁰ Wallis, *Combating Air Terrorism*, p. 27.

³¹¹ Given the discovery of bomb manufacturing in Germany, experts agreed that the warning had constituted a detailed threat: Wallis, *Combating Air Terrorism*, pp. 27-28.

³¹² Wallis, *Combating Air Terrorism*, p. 28.

³¹³ Wallis, *Lockerbie*, p. 109.

³¹⁴ Wallis, *Combating Air Terrorism*, p. 31.

³¹⁵ Wallis, *Lockerbie*, p. 109.

³¹⁶ Wallis, *Lockerbie*, p. 23.

All checked-in baggage, whether it has been screened by X-ray machine or not, should be personally matched and identified with the passengers boarding an aircraft. Any baggage which is not so identified should be off-loaded. This is advisable as examination of the baggage with the help of an X-ray machine has its own limitations and is not fool proof. Some explosives hidden in Radios, Cameras etc. may not be readily detected by such a machine. In fact an explosive not placed in a metallic container will not be detectable by an X-ray machine. Similarly, a plastic explosive can be given an innocuous shape or form so as to avoid detection by an X-ray. Reliance on an X-ray machine alone may in fact provide a false sense of security.³¹⁷

As in 1985, the X-ray equipment used in 1988 was of limited value. It provided only black and white images and required skilled operators.³¹⁸ Wallis wrote that the operator on duty for Pan Am on December 21, 1988, had received no training on the equipment, had not been provided with the machine's operating manual, and had not been tested on his ability to interpret images on the screen. Earlier in the year he had been employed as a cleaner for Pan Am. He had poor eyesight and used his glasses only when he wanted to see detail more clearly. Like all screening staff working for Alert Management, he had not been made aware of the Toshiba cassette radio bomb warning and had received no special instruction on bomb identification.³¹⁹

Wallis stated that Pan Am was, moreover, informed that the bombs recently discovered in Germany would be difficult, if not impossible, to detect by X-ray. Tests conducted at the time demonstrated that the equipment was unable to detect the plastic explosives contained within the cassette radio bombs found by police³²⁰:

By August 1988, knowledge that terrorists had improved technology for the construction of improvised explosive devices (IEDs) designed for use against aircraft was becoming available. Modifications in the manufacture of these bombs [were] coupled with changes in the method of their concealment. It had become obvious that detailed baggage search techniques would be necessary to detect the devices, since X-ray examination was known to be inadequate for the purpose. Nor was the average screening operator considered up to the task of identifying the high-tech detonation mechanisms now available to the terrorists. The FAA

³¹⁷ Exhibit P-164, p. 173.

³¹⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4517.

³¹⁹ Wallis, *Lockerbie*, p. 116.

³²⁰ Wallis, *Lockerbie*, p. 23.

requirement for all baggage to be matched with passengers took on even greater importance.³²¹

Wallis concluded that, despite its knowledge about the lack of utility of X-ray equipment in the current threat situation, Pan Am did not revert to passenger-baggage matching.³²² It chose to use X-ray equipment as its sole security control for interlined baggage.³²³

Following the bombing, a Scottish Fatal Accident Inquiry confirmed that the improvised explosive device consisted of Semtex-type plastic explosive concealed in a Toshiba cassette radio carried in a suitcase.³²⁴ The inquiry also concluded that "...limitations of X-ray screening as a means of detecting plastic explosives contained in electronic equipment were generally recognized" by December 1988,³²⁵ and that reliance by Pan Am on X-ray screening alone for interlined baggage in London and Frankfurt was a "defect" which contributed to the deaths.³²⁶

The US Commission established in 1989 also concluded that the bombing of Flight 103 was preventable:

Stricter baggage reconciliation procedures could have stopped any unaccompanied checked bags from boarding the flight at Frankfurt.³²⁷

Echoing the words of the ICAO Council President two months before the bombing, the report called passenger-baggage reconciliation "...the bedrock of any heightened civil air security system."³²⁸

2.3.2 Air India and Pan Am: Parallel Systemic Failures

The need for passenger-baggage reconciliation as a primary security defence against in-flight bombings was one of the key lessons of the loss of Air India Flight 182, but a narrow focus on this ignores other security weaknesses. In 1985, the failure of Air India to institute this measure, and of the Government of Canada to require it, was symptomatic of major systemic security deficiencies in aviation which, in combination, created an environment vulnerable to sabotage. These deficiencies have been the subject of much of the Commission's focus during its review of aviation security.

³²¹ Wallis, *Lockerbie*, p. 20.

³²² Wallis, *Lockerbie*, p. 23.

³²³ Wallis, *Combating Air Terrorism*, p. 31; see also Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4517-4518.

³²⁴ Wallis, *Lockerbie*, p. 55.

³²⁵ Wallis, *Lockerbie*, p. 56.

³²⁶ Wallis, *Lockerbie*, p. 56.

³²⁷ Wallis, *Lockerbie*, p. 46.

³²⁸ Wallis, *Combating Air Terrorism*, p. 33.

The US Commission's report was critical of both Pan Am and the FAA. It stated that Pan Am's apparent security lapses and the FAA's failure to enforce its own regulations followed a pattern that had existed for months before the bombing and that continued for nine months after.³²⁹ Although the FAA was instrumental in helping ICAO develop new rules after the bombing of Flight 182, the FAA did not effectively monitor their implementation. Despite audits of Pan Am security operations at Frankfurt,³³⁰ the FAA was unaware that Pan Am had stopped matching passengers with baggage at Frankfurt and Heathrow airports.³³¹ Pan Am was also never cited for other breaches of the federal security program. In October 1988, the FAA inspector responsible for overseeing civil aviation security measures in Frankfurt recorded several failures by the airline, including the absence of any identifiable tracking system for interline baggage. He made recommendations to overcome these shortcomings, but did not cite the airline for violating FAA baggage security requirements. Instead, the inspector's report concluded that the minimum FAA requirements were being met.³³²

The Scottish Fatal Accident Inquiry also concluded that the direction and circulars provided to airlines by the UK Department of Transport "...afforded insufficient protection against the possibility that an undetected unaccompanied bag would be transferred"³³³ from the Frankfurt feeder flight to the Boeing 747 at Heathrow. Wallis remarked on the significance of this finding:

Many government civil aviation officials around the world have been apt to issue directives with little or no effort being made to ensure their terms are understood. Monitoring implementation of the regulations is nonexistent. Often the rules are put together by civil servants who have no practical experience of airline or airport operations and are developed without consultation with aviation operations executives. [The Scottish Inquiry's] comments might bring home to government authorities the need to understand the operation and the conditions under which regulations have to be applied before drying the ink on a new set of administrative requirements.³³⁴

While effective oversight by government is crucial for ensuring a properly functioning regime, security is a shared responsibility.³³⁵ It is an integrated system that involves government departments and agencies, as well as private sector and non-profit entities.³³⁶ All stakeholders are obligated to respect the rules that apply to them, and must faithfully discharge their responsibilities. Anything less

³²⁹ Wallis, *Lockerbie*, pp. 45-46.

³³⁰ Wallis, *Lockerbie*, pp. 46-47.

³³¹ Wallis, *Lockerbie*, p. 82.

³³² Wallis, *Lockerbie*, pp. 46-47.

³³³ Wallis, *Combating Air Terrorism*, p. 36.

³³⁴ Wallis, *Combating Air Terrorism*, p. 37.

³³⁵ Exhibit P-361, Tab 1, p. 8.

³³⁶ Exhibit P-169, p. 31 of 202.

than this destroys the value of a legislated regime. Any weakness gives terrorists the chance to exploit the system – a danger clearly demonstrated in the Pan Am bombing. US airlines at the time generally did not favour requiring positive passenger-baggage matching,³³⁷ despite knowing the threat of bombs being placed in unaccompanied baggage. Some airlines were granted permission to use X-rays in place of reconciliation procedures at airports that were not designated as “extraordinary risk.” Frankfurt airport, however, was designated as extraordinary risk.³³⁸

Air carriers play a vital role in ensuring passenger protection. Not only must they adhere strictly to the regime under which they are operating but “...regardless of rules laid down by governments, the carriers themselves need to ensure that their procedures are commensurate with the prevailing threats and risks.”³³⁹

As noted earlier, the Pan Am station in Frankfurt relied on ineffective technology to screen baggage rather than on the established method of baggage-passenger reconciliation. This was similar to the situation in 1985, when Air India relied on technology that was known to be ineffective because it was deemed to be more efficient than the time-consuming and costly passenger-baggage matching process. Air India took this course of action, despite testing that had revealed the PD-4 sniffer to be incapable of detecting explosives, and despite knowing of the limited value of X-ray equipment in explosives detection.³⁴⁰ When the X-ray machine malfunctioned in Toronto on June 22, 1985, screening officers received only cursory, on-the-spot training about the PD-4 equipment, which was then used to check the remaining unscreened baggage.³⁴¹

As early as 1986, an Israeli security consultancy firm had suggested in a report commissioned by Pan Am that the airline was placing too much reliance on technology. The report described the airline’s security operations at European airports as “dangerously lax”³⁴² and criticized the airline’s heavy reliance on technical equipment. The report noted that, under the current program, Pan Am was “highly vulnerable to most forms of terrorist attack.” That Pan Am had not already suffered a major disaster was “merely providential.”³⁴³ The report attacked the air carrier’s management structure, its selection of staff, the lack of adequate training for security employees and the absence of monitoring programs.³⁴⁴ The report declared the entire operation not cost-effective, but did not view an increase in budget as necessary. Rather, all that was required was proper “authority, management and resolve.”³⁴⁵

³³⁷ Wallis, *Lockerbie*, p. 13.

³³⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4516.

³³⁹ Wallis, *Combating Air Terrorism*, p. 37.

³⁴⁰ Exhibit P-436, pp. 31-32.

³⁴¹ Exhibit P-436, p. 31.

³⁴² Wallis, *Lockerbie*, p. 30.

³⁴³ Wallis, *Lockerbie*, p. 30.

³⁴⁴ Wallis, *Lockerbie*, p. 30.

³⁴⁵ Wallis, *Lockerbie*, p. 31.

In the case of Pan Am, the breach in security involved, as noted, a former chief of security of an airline. He gained access to restricted areas of the airport in Malta, enabling the baggage containing the bomb to circumvent normal security procedures altogether. According to Wallis, this "...portrayed the worst possible scenario facing legitimate governments with respect to attacks against civil aviation targets, namely direct involvement (rather than coercion) of airline staff with knowledge of and access to attack aircraft under cover of their legitimate roles."³⁴⁶ He noted that this was not the first civil aviation security incident of this nature.³⁴⁷ This highlights the importance of ensuring adequate security measures for airside and restricted areas of airports, and the need for international co-operation to ensure consistent security throughout. A weakness in security in one location can surreptitiously weaken security at another, whether in the same country or abroad.

Good security must have multiple, robust layers. It must be based on a proper understanding of risk – including an in-depth knowledge of past threats and their current relevance – and it requires the co-operation and collaboration of many entities in Canada and abroad.

It is telling that an exact repeat of the Air India bombing could occur in a field – aviation security – often criticized for "fighting the last war instead of the next."³⁴⁸ The evidence suggests that neither the last war nor the next have been fully addressed, leaving unacceptable gaps in security. Indeed, the Commission has concluded that many of the lessons from 1985 have yet to be incorporated into the domestic regime.³⁴⁹ While Canada immediately championed passenger-baggage reconciliation following the Air India disaster,³⁵⁰ passengers remain vulnerable to sabotage because bombs can still be introduced onto aircraft by means other than passengers and their baggage.³⁵¹

2.3.3 Responses to the Bombing of Pan Am Flight 103

The bombing of Air India Flight 182 was the deadliest single aviation terrorism incident to that time, killing even more than the sabotage of Pan Am Flight 103 three years later. However, as the experts who appeared before the Commission observed, the loss of Pan Am Flight 103 generated a greater sense of collective urgency on the world stage and more support for systemic change. Emphasis was placed on the very same issues that had been raised after the loss of Flight 182, such as hold bag screening (HBS) and air cargo security. Many countries, particularly in Europe, demonstrated a greater commitment to following through with these initiatives.³⁵² Yet earlier work by ICAO, IATA and the Kirpal Commission following the Air India disaster had reached the same conclusion

³⁴⁶ Wallis, *Lockerbie*, p. 38.

³⁴⁷ Wallis, *Lockerbie*, p. 38.

³⁴⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4646.

³⁴⁹ See Section 3.8, which reviews the major deficiencies that still remain in the Canadian regime.

³⁵⁰ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4755.

³⁵¹ Deficiencies in air cargo and airside security continue to provide an avenue by which bombs can be introduced aboard passenger aircraft. See Sections 3.8.1 and 3.8.2 for further details.

³⁵² Exhibit P-166, p. 6.

as the later US and Scottish investigations into the Pan Am bombing – that passenger-baggage reconciliation was the key security measure for preventing bombs in baggage from being placed aboard aircraft.³⁵³

Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the Commission hearings, represented Canada on ICAO's Aviation Security Panel of Experts after the bombing of Flight 103. He participated in similar meetings across Europe for Transport Canada and was uniquely positioned to observe the response as it unfolded. He described as "striking" the attention that many governments paid to the need for widespread enhancements in civil aviation security following the Pan Am tragedy. A series of action plans were developed, with the UK playing a lead role within ICAO to promote broad improvements.

By early 1989, the UK government had made eight proposals to ICAO.³⁵⁴ Among them was a proposal dealing with passenger-baggage reconciliation,³⁵⁵ a measure that ought to have been fully addressed in the wake of the Air India bombing. The adoption of passenger-baggage reconciliation as a mandatory standard for international flights was foremost among the changes made to Annex 17 after the loss of Air India Flight 182. Although an initial implementation date was set for December 19, 1987, the date was changed to April 1989 to allow Contracting States time to comply. However, states that could implement the standard sooner were strongly urged to do so. Still, even by the 1990s, only a few states had begun implementing passenger-baggage reconciliation.³⁵⁶

A further UK proposal called for full HBS of all checked baggage with explosives-detecting equipment. The technology available in 1989, like that of 1985, lacked sophistication. Marriott testified that much of the drive to invest significant resources in research and development for HBS could be traced to the aftermath of Pan Am Flight 103,³⁵⁷ although the same need had been identified earlier following the Air India bombing. Technologies were in development before 1988, but the Pan Am disaster led to an increase in this activity.³⁵⁸ Marriott remarked that:

...[T]he task of integrating [hold] baggage screening systems into airport baggage handling systems was one that received a great deal of engineering attention.... [T]he events of the Pan Am 103 tragedy drove a great many governments, the international community, to focus a great deal more attention on the enhancement of aviation security across the whole range of theme areas, but [hold] bag screening certainly was...[a] principal focus....³⁵⁹

³⁵³ Wallis, *Combating Air Terrorism*, pp. 33, 35.

³⁵⁴ Exhibit P-157, p. 89 of 135.

³⁵⁵ Exhibit P-157, p. 89 of 135.

³⁵⁶ While standards are mandatory, Contracting States can withdraw from their obligations by informing ICAO of their inability or unwillingness to comply: Exhibit P-157, pp. 89-90 of 135.

³⁵⁷ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4520-4521.

³⁵⁸ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4521.

³⁵⁹ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4521.

Some countries, including the UK, managed to implement 100 per cent HBS fairly quickly, but many others, including Canada,³⁶⁰ did not do so until the ICAO standard took effect on January 1, 2006.³⁶¹

The UK also aggressively pursued enhancements to air cargo security after the Pan Am bombing.³⁶² Following the loss of Air India Flight 182, air cargo security had been singled out by the international community as a significant vulnerability.³⁶³ Much like hold baggage, air cargo was becoming an increasingly easy vehicle for getting bombs aboard passenger aircraft.³⁶⁴ Nonetheless, efforts to improve security measures for air cargo did not gain widespread support until 1989, after the bombing of Pan Am Flight 103. By 1990, the US and the UK had joined forces with IATA to promote greater security for air cargo throughout its supply chain. The concept of the “known shipper”³⁶⁵ (the term was later changed to “regulated agent”),³⁶⁶ in which a shipper or consolidator would be licensed by the government after meeting certain security standards, and which was introduced after the Air India bombing, was finally accepted by ICAO in 1991 for addition to Annex 17.³⁶⁷ The UK moved quickly to implement the measure, developing regulations by 1993.³⁶⁸ Canada, on the other hand, has only recently considered measures to strengthen air cargo security in conformity with the ICAO principle.³⁶⁹

The UN Security Council and General Assembly also weighed in on efforts to address the failings that led to the destruction of Pan Am Flight 103. In June 1989, recognizing the difficulty in detecting plastic explosives such as those used in the Pan Am attack, the UN Security Council passed Resolution 635. The Resolution urged ICAO “...to intensify its work on devising an international regime for the marking of plastic and sheet explosives for the purpose of detection.”³⁷⁰ The UN General Assembly subsequently affirmed this resolution. In response, ICAO drafted the *Convention on the Marking of Plastic Explosives for the Purpose of Detection* (1991). The Convention prohibits the manufacture, sale or possession of plastic explosives, commonly used in air terrorism, without specific chemical markings stipulated by the Convention.³⁷¹ Chemical markers

³⁶⁰ Exhibit P-169, p. 65 of 202.

³⁶¹ Exhibit P-157, p. 89 of 135.

³⁶² Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4529.

³⁶³ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4480-4481; Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

³⁶⁴ Exhibit P-162, p. 4; see also Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4480-4481.

³⁶⁵ This term, as it is used in Canada, does not correspond to the meaning attributed to it by Annex 17. In Canada, the term “known shipper” is not a government-licensed shipper or consolidator, but an entity that is known to an airline because a business relationship has been established. See Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4630; see also Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5002-5003.

³⁶⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

³⁶⁷ Wallis, *Combating Air Terrorism*, p. 78.

³⁶⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

³⁶⁹ See, for example, Exhibit P-189; see also Section 3.8.1 for a more detailed analysis of air cargo security in Canada.

³⁷⁰ Exhibit P-157, p. 90 of 135.

³⁷¹ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4228.

in plastic explosives make it easier for electronic equipment and explosives detection dogs to identify them. The Convention entered into force in 1998.³⁷²

The Pan Am bombing prompted Canada to address even more vigorously several systemic security issues exposed following the loss of Air India Flight 182. This included a new emphasis on HBS. Research and development in technology for screening hold baggage for explosives was expedited, with bilateral and trilateral agreements involving Canada, the US and the UK. Transport Canada also accelerated its “foreign offshore security inspection program” to ensure compliance monitoring and quality control, particularly for passenger-baggage reconciliation. In general, the inspection program was meant to ensure that foreign-registered and domestic air carriers departing from foreign airports were implementing Canadian regulatory requirements.³⁷³

The US reacted to the Pan Am bombing by working within international organizations, including ICAO, to improve aviation security worldwide. It also worked with certain countries individually to address specific issues or threats, and examined its own security framework. In May 1990, the US Commission that reviewed the Pan Am disaster made 64 recommendations, among them to:

- transfer primary responsibility for aviation security from US air carriers to the US State Department;
- ensure mandatory criminal record checks for all airport employees;
- conduct mandatory passenger-baggage reconciliation; and
- create a technical assistance program, through the FAA, to provide aviation security assistance to countries upon request and to concentrate efforts wherever the threat was greatest.³⁷⁴

The CATSA Act Review Advisory Panel (CATSA Advisory Panel), the independent panel of experts that, as part of its mandate, reviewed aviation security issues associated with the bombing of Air India Flight 182, reported that many of the US Commission’s recommendations were not implemented. Ironically, this failure flowed, at least in part, from industry concerns about the cost of funding security initiatives and the impact they would have on their operations.³⁷⁵ One influential family member of a victim of the Pan Am bombing later argued that “...history has proven the aviation industry’s lack of sincerity and willingness to address safety and security on behalf of their customers.”³⁷⁶

³⁷² Canada incorporated the requirements of the Convention through amendments to the *Explosives Act*, which came into force on September 11, 1996. See Exhibit P-157, p. 90 of 135, note 113; see also Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4228.

³⁷³ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4528.

³⁷⁴ Exhibit P-157, p. 90 of 135

³⁷⁵ Exhibit P-157, p. 90 of 135.

³⁷⁶ Victoria Cummock, who was appointed as a Commissioner on the subsequent 1996/7 White House Commission on Aviation Safety and Security to investigate the loss of another Boeing 747, TWA Flight 800, later made these remarks in a letter of dissent to the report of that Commission: Wallis, *Lockerbie*, p. xiv.

In his 2001 book, *Lockerbie: The Story and the Lessons*, Wallis noted that US aviation security standards were still not optimal then and that passengers remained vulnerable to the baggage bomber.³⁷⁷ He contended that it was not just a “lack of sincerity and willingness” on the part of air carriers, but also that, despite the best efforts of ICAO, IATA and other international bodies, many national authorities failed to understand what was required of them. He also laid blame on the inadequate funding pledged to civil aviation security.³⁷⁸ The CATSA Advisory Panel noted that, even when governments and other organizations worked together after the Pan Am bombing to improve and standardize security measures around the world, many measures proposed by ICAO remained either voluntary or were not adopted by member states.³⁷⁹

Transport Canada officials considered the bombing of Pan Am Flight 103 to be the second watershed in civil aviation security, with Air India Flight 182 being the first.³⁸⁰ However, Wallis considered the Pan Am bombing merely to represent a failure to respond to the lessons of Air India Flight 182.³⁸¹ The loss of Pan Am Flight 103 simply demonstrated that the Air India disaster had not resonated with the international community as a whole.

2.3.4 Failure to Appreciate Significance of Air India Flight 182 Bombing

The bombing of Flight 182 was a seminal moment in the history of civil aviation security. Within days, emergency meetings were held at IATA and ICAO. Airline security chiefs and authorities came from around the world to discuss how to address major security deficiencies.³⁸² The bombing triggered a major overhaul of international civil aviation security. As well, the Kirpal Commission in India conducted a thorough investigation of the incident, producing an extensive report in 1986. The report made key recommendations directed at ICAO, national authorities, airlines and airports.³⁸³ Had these recommendations been followed, terrorists might not have succeeded in bombing Pan Am Flight 103 in 1988.

Experts who appeared before the Commission agreed that, although the Air India bombing was one of the most significant acts of unlawful interference with civil aviation, it was only the loss of Pan Am Flight 103 that led to more definitive action on the very same security issues.³⁸⁴ The bombing of Flight 103 resulted in a significant increase in dialogue internationally about civil aviation security.³⁸⁵ However, the question remains: Why did the earlier Air India bombing not have greater impact on aviation officials, even when they faced a specific threat of sabotage?

³⁷⁷ Wallis, *Lockerbie*, pp. 150-151.

³⁷⁸ Wallis, *Lockerbie*, pp. 151-152.

³⁷⁹ Exhibit P-157, p. 91 of 135.

³⁸⁰ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4510.

³⁸¹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4210.

³⁸² Exhibit P-162, pp. 2-3, 13.

³⁸³ Exhibit P-164, pp. 172-175.

³⁸⁴ See, for example, Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4525.

³⁸⁵ Exhibit P-166, p. 6.

The CATSA Advisory Panel suggested that the loss of Flight 103 merely three years after the Air India bombings had "...resulted in a dramatic loss of public confidence in civil aviation and further pressured governments into taking action."³⁸⁶ However, the Commission heard evidence suggesting that the different treatment of virtually identical incidents cannot be entirely explained by this public outrage.

Both Wallis and St. John highlighted the symbolism that the attack against Pan Am Flight 103, an American flag carrier, created. The Pan Am bombing killed all of the mostly American passengers and crew.³⁸⁷ It was seen as a calculated act of aggression against the US.³⁸⁸ Both the fact that it was an American aircraft and that "enemies in the Middle East" caused the crash, ensured extensive media coverage, particularly in the US.³⁸⁹ Air India, on the other hand, was the flag carrier for India. When Flight 182 was destroyed, India, not Canada, was the target. The bombing of Flight 182 did not create the same sort of imagery as the Pan Am attack.³⁹⁰

Shortly after the Pan Am bombing, it was widely believed that the attack was retaliation for a tragic accident in which an American warship, the USS Vincennes, mistakenly shot down an Iran Air Airbus "full of pilgrims."³⁹¹ More than 200 passengers and crew died after their aircraft was struck by a surface-to-air missile.³⁹² Ultimately, however, responsibility for the Pan Am bombing was attributed to a Libyan, not Iranian, operative. The subsequent imposition of sanctions on Libya by the US served to maintain the Pan Am bombing as a live international issue.³⁹³

As well, another event overshadowed the Air India bombing for the American public and the US civil aviation community. This was the seizure of an aircraft belonging to Trans World Airlines (TWA), an American airline, on June 14, 1985,³⁹⁴ and the subsequent saga of hostages held in Lebanon. The lessons of the Air India disaster were overlooked – a profound mistake, according to Wallis:

The importance given by the U.S. carriers to the TWA seizure was understandable. It was a major national and media event with daily pictures of the aircraft on the ground at Beirut being shown on all the front pages and on the television news bulletins. ... With a number of men taken and held hostage in Beirut, the level of emotion created in the United States was certain to give precedence of thought in that country to this

³⁸⁶ Exhibit P-157, p. 89 of 135.

³⁸⁷ Exhibit P-157, p. 89 of 135.

³⁸⁸ Testimony of Peter St. John, vol. 37, May 31, 2007, p. 4522; see also Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4526; see also Wallis, *Lockerbie*, p. 53.

³⁸⁹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4525-4526.

³⁹⁰ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4527.

³⁹¹ Testimony of Peter St. John, vol. 37, May 31, 2007, pp. 4522-4523.

³⁹² Wallis, *Combating Air Terrorism*, p. 28.

³⁹³ Testimony of Peter St. John, vol. 37, May 31, 2007, pp. 4522-4523.

³⁹⁴ Wallis, *Combating Air Terrorism*, p. 2.

criminal act rather than to the Air India incident. Yet it was a gargantuan mistake for the Air India disaster to be afforded only second-level importance by the U.S. airlines. From the loss of the *Kanishka* came the most significant change in international aviation security standards in the 1980s – the mandatory requirement for passenger and baggage reconciliation. Failure by Pan Am to implement this procedure was to claim 270 more lives just three years later.³⁹⁵

Wallis speculated that, had US airlines participated more fully in the debates within IATA that followed the Air India bombing, their attitudes towards passenger-baggage reconciliation might have been different.³⁹⁶ Passenger and baggage matching had been recommended by IATA since the summer of 1985. The Kirpal Commission urged the same measure in its February 1986 report, particularly for interlined baggage.³⁹⁷

Wallis also noted that the Pan Am disaster, unlike the bombing of Air India Flight 182, occurred over land. The wreckage was strewn over the town of Lockerbie and people also died on the ground: "...The hunt for wreckage, for evidence as to what had happened, the attempt to recover the victims" was all on dry land and was "played out on television."³⁹⁸ In contrast, Flight 182 crashed into the sea, and although the hunt for wreckage received media coverage, the extent of the damage was not as easily visible.³⁹⁹

However, it was perhaps the perception that the bombing of Pan Am Flight 103 was an attack on the West, rather than on the East, that lies at the heart of the issue. As St. John observed in testimony, the downing of an American airline containing mostly British and American passengers created "...enormous consternation and international reaction."⁴⁰⁰

Some other civil aviation security incidents give rise to similar inferences. On November 29, 1987, liquid explosives carried in hand baggage destroyed Korean Air Flight 858 as it flew over the Andaman Sea, destined for Seoul. All 115 people on board died. South Korea was the target.⁴⁰¹ This was clearly a significant act of aviation terrorism, but the threat posed by liquid explosives was not addressed by the international community until 2006, when a terrorist plot was exposed in the UK to launch simultaneous attacks on several Western air carriers using liquid and gel explosives. Only then were lasting security measures implemented. A ban on liquids and gels in carry-on baggage occurred, and limits on the volumes of liquids and gels are now a feature of pre-board screening (PBS).⁴⁰²

³⁹⁵ Wallis, *Lockerbie*, pp. 10-11.

³⁹⁶ Wallis, *Lockerbie*, p. 13.

³⁹⁷ Exhibit P-164, Recommendation 5.5, p. 173.

³⁹⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4525.

³⁹⁹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4525.

⁴⁰⁰ Testimony of Peter St. John, vol. 37, May 31, 2007, p. 4522.

⁴⁰¹ Wallis, *Combating Air Terrorism*, p. 18.

⁴⁰² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585.

No country, air carrier or airport operator can afford to ignore aviation security incidents, wherever in the world they occur. A threat to one must be understood as a threat to all.

2.3.5 Conclusion

Security can never be perfect, but there is no excuse for repeating mistakes when the measures to prevent them are known and available. The bombing of Air India Flight 182 spurred the civil aviation community to action to prevent sabotage. The introduction of a regulation requiring passenger-baggage reconciliation was a known method of preventing a recurrence of this disaster. Federal regulations in the US required its use. Yet Pan Am did not implement the measure for its Flight 103.

Perhaps the greater focus on the Pan Am bombing reflected the US-centred axis of world media. Within the civil aviation security community itself, this bias should not have carried weight. The lessons from the bombing of Air India Flight 182 should have been absorbed into the marrow of that community. The follow-up lesson taught by Pan Am Flight 103 should not have been necessary before the security gaps already identified after the Air India bombing were addressed.

The CATSA Advisory Panel noted that, even after the Air India and Pan Am bombings, the implementation of many measures proposed by ICAO remained voluntary and that, even when the measures were mandatory, Contracting States did not always adopt them. Before September 11, 2001, few governments had introduced regulations requiring the screening of all passengers and hold baggage on all flights. Few countries conducted passenger-baggage reconciliation, and equipment for detecting plastic explosives at airports was relatively rare.

Words and pledges of action are not enough. Improved security conceived in theory is fine, but the practical application is the only thing that will save lives. Aviation authorities around the world must commit in concert to an unfaltering focus on effective security. If weaknesses are allowed here and there, terrorists will simply direct proven methods of sabotage to these points of vulnerability.

VOLUME FOUR

AVIATION SECURITY

CHAPTER III: CIVIL AVIATION SECURITY IN THE PRESENT DAY

3.1 Responses to the Terrorist Attacks of September 11, 2001

On September 11, 2001, four American passenger jets were hijacked in a coordinated terrorist attack. Two were flown into the twin towers of the World Trade Center in New York City. The third aircraft struck the Pentagon building in Arlington, Virginia, while the fourth, possibly destined for an attack on the White House, crashed into a field southeast of Pittsburgh, Pennsylvania.¹

These attacks represented a fundamental change in aviation terrorism. Never before had aircraft been successfully used as guided missiles in a sophisticated suicide mission.² Existing measures for aviation security proved ineffective.³ Canadian aviation security underwent its most significant change as a result of these attacks.⁴

3.1.1 Historical Context

There was a popular misconception that this was the first time terrorists had orchestrated an incident using multiple aircraft. In fact, the first coordinated incident involved Dawson's Field, an abandoned airstrip in the Jordanian desert, some 30 years earlier. It was organized by Leila Khaled, a prominent leader within the Popular Front for the Liberation of Palestine (PFLP). The group planned to hijack three aircraft, representing different countries and departing from different locations, and then direct them to Dawson's Field.⁵

On September 6, 1970,⁶ members of the group successfully took over a Swissair Coronado aircraft and a Trans World Airlines (TWA) 707 and flew them to Dawson's Field. The plan also included an attack on an El Al aircraft, which involved Khaled herself. She flew from Germany with a fellow PFLP member and they transferred to the El Al flight in Amsterdam. Two others were to join them on this mission, but the flight was overbooked and the two were unable to secure seats. Instead,

¹ Bob Rae, *Lessons to be Learned: The report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Secretariat, 2005), p. 42 [*Lessons to be Learned*].

² Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4532; see also Exhibit P-157, p. 93 of 135.

³ Exhibit P-157, p. 93 of 135.

⁴ Exhibit P-169, p. 16 of 202.

⁵ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4530.

⁶ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

they seized a Pan American (Pan Am) Boeing 747 and flew it to Cairo, where the aircraft was destroyed by explosives following its evacuation.⁷

Although Khaled and her companion continued with their El Al hijacking plans, they were unsuccessful. Guards on board the El Al flight intervened, her companion was shot and Khaled was taken into custody in London, the destination to which the aircraft had been diverted. In immediate response, other members of the PFLP hijacked a British Overseas Airways Corporation (BOAC) aircraft, and it joined the other commandeered planes at Dawson's Field. About 300 hostages were held in the desert during negotiations for the release of terrorists detained in several European countries. The terrorists achieved their objectives and the passengers were released unharmed.

This was a highly successful coordinated terrorist attack.⁸ It is generally considered to represent the birth of modern air terrorism.⁹

The terrorists in the Dawson's Field incident wanted to make a political statement, but they also wanted to emerge alive, unlike those involved in the events of September 11th.¹⁰ The civil aviation community had considered the possibility of terrorists seizing and exploding aircraft over major world capitals with the intent of "raining terror from the skies."¹¹ Even so, the "disposable" terrorist who sacrificed his or her life in the attack was not considered a serious possibility before 2001.

In 1994, terrorists attempted to explode a hijacked aircraft over Paris, but authorities foiled the plot.¹² The prospect of planes being flown into critical infrastructure buildings was raised in the United States as early as 1972. On November 10, 1972, Southern Airways Flight 49 was seized by three fugitives in a lengthy hijacking. At one point, the hijackers threatened to crash the aircraft into an atomic power plant in Oak Ridge, Tennessee.¹³

⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4530-4531; see also Exhibit P-448, pp. 70-71.

⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4531.

⁹ Exhibit P-259: Rodney Wallis, *Combating Air Terrorism* (New York: Brassey's, 1993), p. 92 [Wallis, *Combating Air Terrorism*].

¹⁰ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4531.

¹¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4532.

¹² On December 24, 1994, Air France Flight 8969, bound for Paris from Algiers, was hijacked by the Algerian terrorist organization Armed Islamic Group (GIA). The four hijackers boarded the aircraft disguised as Air Algérie security staff. Authorities delayed departure of the aircraft, but were intimidated into giving the go-ahead when the hijackers killed two of the 227 persons on board. The French government decided not to allow the aircraft to approach Paris because its consulate in Oran, Algeria had received an intelligence warning that the hijackers intended to explode the aircraft over Paris. The flight crew convinced the hijackers that refueling in Marseille was required. After the aircraft touched down, hours of negotiations ensued, whereupon the terrorists demanded fuel. French police commandos (GIGN) stormed the aircraft and after a 20-minute gunfight successfully rescued the 161 remaining passengers (some had been released during negotiations) and three flight crew. This method of air terrorism was discussed among aviation security circles for some time afterwards. See Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4532; see also Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹³ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

Successful suicidal hijackers were also not completely unheard of before the September 11th attacks. On December 10, 1987, a disgruntled former US Air employee hijacked a US Air aircraft. He shot the pilot, sending the aircraft into a dive and crash that left no survivors among the 43 people on board.¹⁴ Suicide-for-insurance schemes were a feature of aviation sabotage in the 1950s and 60s.¹⁵ These incidents, however, involved “the fringe element”¹⁶ – suicidal individuals with isolated agendas – whose behaviour was random and very different from that of “...a group of people planning and carrying out a mass attack.”¹⁷ Aviation security measures should of course be designed to protect against both suicidal individuals and those intent on carrying out a mass attack.

3.1.2 International Response

The international civil aviation community reacted swiftly to the events of September 11th. In the following months, the International Civil Aviation Organization (ICAO) passed several resolutions strongly condemning the use of aircraft as weapons of mass destruction.¹⁸ It also called upon aviation security specialists to bring focus to what some described as the “new post-9/11 threat level.”¹⁹ An urgent review of Annex 17 to the *Convention on International Civil Aviation* (“*Chicago Convention*”) began. Annex 17 set out the basis for the ICAO civil aviation security program. The review led to the tenth amendment to Annex 17. Amendment 10 was a major revision,²⁰ introducing many new standards to strengthen security overall and to respond directly to the September 11th attacks.²¹

In the autumn of 2002, ICAO introduced a mandatory program for auditing state compliance with Annex 17 standards known as the Universal Security Audit Program (USAP).²² Annex 17 was further amended by Amendment 11 in April 2006. Amendment 11 clarified the wording of some provisions and significantly raised the standards for screening passengers, baggage and cargo. This amendment is the most current security standard for safeguarding civil aviation.²³

¹⁴ Wallis, *Combating Air Terrorism*, pp. 2-3; see also Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁵ On July 25, 1957, an explosion occurred on Western Air Lines Flight 39 while it was mid-air over the Mojave Desert in Southern California. In what was believed to be a suicide-for-insurance scheme, a retired jeweller had set off dynamite explosives in the lavatory shortly after the flight had taken off. The perpetrator died in the incident, but all others aboard were uninjured. A murder-for-insurance scheme had occurred in Canada several years earlier. On September 9, 1949, near Sault Au Cochon, Quebec, a bomb exploded in a forward baggage compartment of a Quebec Airways (Canadian Pacific) DC-3, killing 23 people. Albert Guay and two accomplices (the bomb maker and the person who delivered the package containing the bomb to the plane) were tried, convicted and executed. Guay's wife, who died in the incident, had been insured, with Guay as the beneficiary. See Exhibit P-448, p. 95; see also Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4534.

¹⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4534.

¹⁸ Exhibit P-157, p. 93 of 135.

¹⁹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4706.

²⁰ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4707.

²¹ Exhibit P-157, p. 93 of 135; see also Exhibit P-180.

²² Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4709.

²³ Exhibit P-157, p. 94 of 135.

3.1.2.1 International Civil Aviation Organization: Annex 17 Amendments

Amendment 10 to Annex 17 was developed by the Aviation Security Panel (AVSEC Panel) of ICAO, which met in the autumn of 2001. The Panel was created after the Air India bombing.²⁴ This group of international civil aviation security experts provides advice to ICAO on the development of Annex 17 standards and recommendations. As it did after the Air India bombing, the AVSEC Panel undertook a comprehensive revision of Annex 17 in 2001.²⁵ Amendment 10, or the Seventh Edition, to Annex 17 was adopted in December 2001 and became effective in April 2002.²⁶ It introduced many new standards to enhance security, both on the ground and in aircraft, including a requirement to ensure the prevention of unauthorized access to the cockpit,²⁷ a direct response to the attacks of September 11th.²⁸ Other new provisions relating to domestic operations were described by one commentator as "...an unprecedented reach by an international organization into domestic law...accomplished through the exercise of the organization's quasi-legislative authority to amend the *Chicago Convention*."²⁹ Provisions dealt with:

- international co-operation regarding threat information;
- the National Aviation Security Committee;
- the appropriate authority;
- quality control;
- access control;
- screening of passengers, carry-on baggage and hold baggage;
- in-flight security personnel;
- code-sharing and collaborative arrangements;
- human factors in civil aviation security; and
- management of responses to acts of unlawful interference.³⁰

In April 2006, Annex 17 was again revised. Amendment 11 set out the current security standards for civil aviation. The amendment clarified the wording of existing standards and included significant improvements to the requirements for passenger, baggage and cargo screening. For example, Standard 4.5.3 strengthened previous provisions implemented by ICAO in 1989³¹ for passenger-baggage reconciliation. Standard 4.5.3 reads as follows:

²⁴ In the immediate aftermath of the Air India and Narita Airport bombings, ICAO convened an *ad hoc* group of security specialists to review Annex 17. It later became a permanent group and was renamed the AVSEC Panel. See Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

²⁵ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4707.

²⁶ Exhibit P-157, p. 93 of 135; see also Exhibit P-180.

²⁷ Exhibit P-157, p. 93 of 135.

²⁸ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4708.

²⁹ See Exhibit P-157, p. 93 of 135, quoting from Paul Dempsey, *Aviation Security: The Role of Law in The War Against Terrorism*, Columbia Journal of Transnational Law, 2006, p. 689.

³⁰ Exhibit P-180, p. viii; see also Exhibit P-157, p. 93 of 135.

³¹ Exhibit P-157, p. 94 of 135.

Each Contracting State shall ensure that commercial air transport operators do not transport the baggage of passengers who are not on board the aircraft unless that baggage is identified as unaccompanied and subjected to additional screening.³²

Hold bag screening (HBS) was addressed in Standard 4.5.5, which required each Contracting State to ensure that:

...commercial air transport operators transport only items of hold baggage which have been individually identified as accompanied or unaccompanied, screened to the appropriate standard and accepted for carriage on that flight by the air carrier. All such baggage should be recorded as meeting these criteria and authorized for carriage on that flight.³³

Amendment 11 also required security controls for cargo and mail before they were loaded onto commercial aircraft.³⁴ New requirements about screening personnel were established, including security clearance procedures, performance standards, certification and recertification, periodic audits, tests, surveys and inspections, and the authority to require remedial actions.³⁵

Amendment 11 required ICAO Contracting States to have in place restricted area clearance systems for authorized personnel, checkpoints to verify their identity on entry to restricted areas and random screening of persons and identification of vehicles entering restricted areas. The relative proportion of these measures was to be based on a risk assessment carried out by the appropriate national authority.³⁶ In addition, Amendment 11 enhanced the security provisions of other Annexes to the *Chicago Convention*, such as the recommended use of biometric data, including face recognition, iris scans and fingerprints in machine-readable travel documents,³⁷ as well as aircraft and airport perimeter security.³⁸

In-flight security measures were addressed in Standard 4.7. These included the handling of disruptive passengers and the provision of armed "in-flight security officers," or air marshals.

In response to the 2006 plot in the UK to bomb several US- and Canada-bound aircraft by using liquid or gel explosives, ICAO expanded its list of items prohibited on aircraft to include liquid, gel and aerosol products. ICAO pledged to deal

32 Exhibit P-157, p. 94 of 135.

33 Exhibit P-157, p. 94 of 135.

34 Exhibit P-157, p. 94 of 135.

35 Exhibit P-157, p. 94 of 135.

36 Exhibit P-157, p. 94 of 135; see also Exhibit P-181, p. 4-1, s. 4.2.

37 Exhibit P-157, p. 95 of 135.

38 See Extracts from Annex 9 – Facilitation and Extracts from Annex 14 – Aerodromes, Exhibit P-181, pp. ATT-4, ATT-10; see also Exhibit P-157, p. 95 of 135.

“proactively” with this and other threats that might emerge. It also promised to focus on enhanced airside security, including screening airport workers, and cargo, catering and hold baggage security, as well as the possible introduction of other security measures, such as behavioural pattern recognition.³⁹

According to the CATSA Act Review Advisory Panel (CATSA Advisory Panel), an independent panel of experts, the two amendments to Annex 17 that were adopted after September 11th reflected the lessons learned from events such as the Air India and Pan Am bombings and the attacks of September 11th. ICAO continues to review and update Annex 17 to address the changing aviation security environment.⁴⁰

3.1.2.2 International Civil Aviation Organization: Universal Security Audit Program

In February 2002, ICAO convened a high-level ministerial conference on aviation security to develop a plan for continued security enhancements. Among the most significant initiatives was the Universal Security Audit Program (USAP).⁴¹ Although the concept of such a program had been discussed at a ministerial-level meeting of ICAO in 1989, the idea did not gain sufficient political support. Issues of national sovereignty hindered progress.⁴² It was not until 13 years later, after the 9/11 attacks, that the 33rd Assembly of ICAO “...reached the same conclusion as the earlier meeting of ministers.”⁴³ Following the high-level ministerial conference in 2002, Canada was invited to participate in a working group to develop the audit program.⁴⁴ Transport Canada’s Director of Security, Jean Barrette, participated. The audit program was launched in the autumn of 2002.⁴⁵

Administered by ICAO, the USAP is an international program for assessing state compliance with Annex 17 standards⁴⁶ through “regular, mandatory, systematic and harmonized audits.”⁴⁷ Under the program, a team of auditors is sent to a state after advance notice from ICAO.⁴⁸ The team evaluates national aviation security at the government level, studying the country’s regulatory structure, including legislation and regulations that pertain to aviation security, to assess the structure’s comprehensiveness and sustainability.⁴⁹ On a sample basis,⁵⁰ the

³⁹ Exhibit P-157, p. 95 of 135.

⁴⁰ Exhibit P-157, p. 95 of 135.

⁴¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4709.

⁴² Exhibit P-261: Rodney Wallis, *How Safe Are Our Skies? Assessing the Airlines’ Response to Terrorism* (Westport, Conn.: Praeger Publishers, 2003), p. 72 [Wallis, *How Safe Are Our Skies?*].

⁴³ Wallis, *How Safe Are Our Skies?*, p. 72.

⁴⁴ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4714-4715.

⁴⁵ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4709.

⁴⁶ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4709.

⁴⁷ Exhibit P-157, p. 93 of 135.

⁴⁸ Advance notice usually consists of a few months. See Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4724.

⁴⁹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4734.

⁵⁰ Wallis, *How Safe Are Our Skies?*, p. 72.

team also examines security and policing of airports and airlines.⁵¹ The audit identifies and helps correct deficiencies in the implementation of Annex 17 security standards and recommendations.⁵² An ICAO manual outlines the audit process and includes a code of ethics. The manual describes the items to be audited, the method for conducting the audit, the process for state notification, and pre- and post-audit briefings. It also covers the selection, training and certification of auditors. The manual is available to all Contracting State members of ICAO.⁵³

The USAP exemplifies collaborative action by ICAO members. This is both its strength and its weakness.

Audit teams are selected by ICAO from a pool of auditors nominated by member states. Typically, these auditors are drawn from national aviation or transportation security administrations. They are public servants with experience in aviation security.⁵⁴ Auditors who participate in the USAP are trained further and certified by ICAO.⁵⁵ Canada contributes regularly to ICAO's pool of auditors. Canadian participants who are ICAO-trained and certified may work under the auspices of the USAP around the world.⁵⁶

A USAP audit of Canada took place in May 2005. According to the agreements signed between ICAO and audited states, USAP findings and recommendations cannot be made public.⁵⁷ The USAP audit report of Canada therefore remains confidential. Nevertheless, at least three independent national reviews of Canada's aviation security, both before and after the USAP audit, identified significant and ongoing deficiencies. The reports include *The Myth of Security at Canada's Airports*,⁵⁸ published in January 2003 by the Standing Senate Committee on National Security and Defence (Senate Committee); *Flight Plan: Managing the Risks in Aviation Security*,⁵⁹ issued in 2006 by the CATSA Advisory Panel; and the *Canadian Security Guide Book*,⁶⁰ an update on airport security released by the Senate Committee in 2007.

The Commission finds that deficiencies in security still have not been addressed sufficiently. Problems that remain include those relating to air cargo security, non-passenger screening and access to airside and restricted areas of airports, as well as Fixed Base Operations (FBOs) and the General Aviation (GA) sector.⁶¹

⁵¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4734.

⁵² Exhibit P-157, p. 93 of 135.

⁵³ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4716. As of April 2009, there were 190 Contracting States of ICAO.

⁵⁴ Testimony of Jim Marriott, vol. 39, June 4, 2007, pp. 4710-4711.

⁵⁵ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4712.

⁵⁶ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4710.

⁵⁷ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4714.

⁵⁸ Exhibit P-171, pp. 41-42, 47-96 of 256.

⁵⁹ Exhibit P-169; see, in particular, pp. 52-56, 57-59, 67-69 of 202.

⁶⁰ Exhibit P-172; see, in particular, pp. 11-44, 65-74 of 155.

⁶¹ See Sections 8.1, 8.2 and 8.3 for further elaboration regarding these deficiencies.

The secretive nature of the USAP audit, in which results are shared only with the state,⁶² raises some concerns, particularly because problems that were raised by others before the audit seemed to persist even after the audit. Rodney Wallis, an international aviation security expert and former Director of Security for the International Air Transport Association (IATA), noted:

...[I]t is an interesting situation, because if we are looking at [the audit] in ignorance and we note that the audit team came, do we assume that the audit team found nothing, and everything was rosy? Do we assume that they found things were wrong, and nothing has been done? And I say nothing has been done because [the Senate Committee] comes along and [is] critical, and I just wonder how the two relate.⁶³

It appears that the USAP audit raised some concerns, because Canada prepared a Corrective Action Plan in response to the audit, and because ICAO made a follow-up visit in 2007 to review Canada's progress on issues that were raised during the 2005 audit.⁶⁴

Transport Canada officials advised the Commission in May 2008 that ICAO had completed a full cycle of audits. In other words, all Contracting States had been audited under the existing USAP. The focus of ICAO audits is now shifting from the scrutiny of aviation security practices at the government and airport level towards a review of the oversight capabilities of states. In future, ICAO will audit each Contracting State's ability to audit its own aviation security regime.⁶⁵

Transport Canada officials praised the USAP, but it received sharp criticism from Wallis. During his time at IATA between 1980 and 1991, Wallis was responsible for a similar international airport survey program, known as the Intensified Aviation Security Program. This program was established in the late 1970s by the Security Advisory Committee (SAC), a specialist committee of IATA. SAC membership consisted of security chiefs of major airlines, and the Committee was led by IATA's Director of Security.⁶⁶ The SAC sought to identify lessons to be learned and it developed collective policies for preventing terrorism. Its members recognized that some airports were more vulnerable than others, since implementation of Annex 17 standards differed widely, and not all governments had adopted the security rules contained in Annex 17. The SAC noted ICAO's inability to secure implementation of its provisions. In response, the SAC developed its Intensified Aviation Security Program,⁶⁷ which involved surveying airports that member airlines identified as problematic.⁶⁸ Sometimes

62 Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4714.

63 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4741.

64 Exhibit P-101 CAF0827, p. 11 of 19.

65 Exhibit P-101 CAF0827, p. 13 of 19.

66 Wallis, *How Safe Are Our Skies?*, p. 69.

67 Wallis, *How Safe Are Our Skies?*, p. 69.

68 Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4717-4718.

airlines would nominate airports to be surveyed because security standards were perceived to be poor. Other times, an airport authority would approach IATA and request a survey. Either way, surveys took place with the full consent of the authority concerned.⁶⁹ Wallis wrote about the benefits of the Intensified Aviation Security Program for airlines:

This was not an altruistic action by the airlines. It was simply a very cost effective way of ensuring that airlines serving a particular airport were afforded the maximum protection against terrorist attacks.⁷⁰

The Council of Europe, in a review of aviation security, declared the IATA program to be the "...only objective survey program available to the industry and to governments."⁷¹

Wallis was responsible for about 200 airport surveys around the world during his time at IATA. He expressed several concerns about the USAP auditing process. First, he noted the considerable delay in establishing the program after it was conceived. ICAO had discussed the possibility of an audit program in 1989, following the bombing of Pan Am Flight 103.⁷² A program to assess state and airport compliance with compulsory security measures would have been understandable in the aftermath of this bombing, since it involved a failure of Pan Am to implement a federally-required passenger-baggage reconciliation program.⁷³ ICAO convened a ministerial-level meeting in 1989, a meeting which included Canada's Minister of Transport and corresponding ministers from the US and the UK.⁷⁴ Those at the meeting referred to IATA's survey activities and recommended starting a voluntary ICAO-based security survey program for states, to be initiated only on state request. Wallis viewed the voluntary nature of the proposed program and the fact that it would come into play only when a state requested as a limitation. Nonetheless, he concluded that, though such a service could have proved valuable, the political nature of ICAO, as discussed earlier, hindered approval of the program.⁷⁵

The 13-year delay in establishing the ICAO audit program highlights a theme that has emerged before the Commission – that it is often not the first major incident that sparks change in security measures, but only the second or third. Only then does a protective measure find acceptance. Examples of measures, besides the USAP and passenger-baggage reconciliation, where implementation or enforcement showed this pattern of delay include full hold bag screening (HBS) and air cargo security initiatives, such as cargo screening and a system

⁶⁹ Wallis, *How Safe Are Our Skies?*, p. 71.

⁷⁰ Wallis, *How Safe Are Our Skies?*, p. 71.

⁷¹ Wallis, *How Safe Are Our Skies?*, p. 72.

⁷² Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4718; see also Wallis, *How Safe Are Our Skies?*, p. 72.

⁷³ Exhibit P-260: Rodney Wallis, *Lockerbie: The Story and the Lessons* (Westport, Conn.: Praeger Publishers, 2001), p.12 [Wallis, *Lockerbie*].

⁷⁴ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4718; see also Wallis, *How Safe Are Our Skies?*, p. 72.

⁷⁵ Wallis, *How Safe Are Our Skies?*, p. 72.

of regulated agents. Air cargo security still has not been properly addressed in Canada.

Wallis questioned the effectiveness of the USAP. He felt the underlying principles were problematic. The survey of airports only on a "sample basis" was of particular concern, since the security of passengers depended upon the security practices of all airports and airlines. He argued that the focus of audits should be on the application of security measures, not merely on the high level organization running the security program.⁷⁶

Wallis was also concerned about how auditors were selected and their level of expertise, particularly since they were drawn from the civil service of their home countries, unlike the experts engaged for the IATA survey program:

One difference between any ICAO program and that of IATA might be in the experience of the teams chosen to undertake the monitoring task. The airline teams were all practicing security professionals with line responsibilities within their own airlines. They had to maximize protection for their companies and its customers. There is a danger the ICAO teams will comprise civil servants, volunteered for the task by individual countries, but who have had no direct, practical aviation security experience at airports or within airlines.⁷⁷

Wallis was concerned that, in an imperfect world, states might not engage in a rigorous process of selection and might nominate persons "...for the simple reason [that] it's somebody[']s turn or some department's turn to have somebody working in an international field. So you can send anybody in effect."⁷⁸ As well, individuals might be selected for the USAP from states that have minimal experience in aviation security. Instead, he said, auditors should be appointed from countries with proven experience and competence in security.⁷⁹

Wallis stated that he was not "in any way" challenging the integrity of individuals nominated by states, but that he was "questioning the practicality of such a structure," since civil servants generally did not have a working knowledge of aviation security at the airport or airline level.⁸⁰ He stated that individuals lacking practical experience in aviation security could not suddenly become competent merely by taking a few weeks' training.⁸¹ In contrast, IATA audit teams consisted of security heads of major airlines who possessed considerable experience with

⁷⁶ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4719.

⁷⁷ Wallis, *How Safe Are Our Skies?*, p. 73.

⁷⁸ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4720.

⁷⁹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4720.

⁸⁰ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4720, 4722.

⁸¹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4723-4724.

their own airlines and with other airlines and airports around the world.⁸² He continued:

You have to have knowledge of another airlines' operation, and I consider the people that have come up through this arena are the true experts capable of monitoring, auditing, identifying problems at airports around the world. They are there to protect their commercial interests in such places. I don't see this with ICAO.⁸³

If auditors lacked this expertise, notifying states of upcoming audits increased the potential for states to devise "cosmetic" solutions to disguise deficiencies in time for the audit. On the other hand, the IATA audit teams, which sought permission to survey airports where problems were already identified, could not be fooled. They were experts in the field and they were auditing airports where industry members had identified many deficiencies. In such cases, auditors could readily detect contrived or cosmetic solutions to security issues.

Wallis described how the IATA survey program was structured in the 1980s. A request for an audit team would usually be made by an industry member. A team of experts would be selected, based on those airlines with direct or planned involvement in a geographic area. The experts would have airline experience and often also a military or police background. The IATA audit teams reviewed eight key security points, beginning at the national level, assessing state compliance with several international conventions, including compliance with Annex 17 provisions. The team would then assess airport security. For example, it would review whether a crisis plan existed for dealing with an instance of unlawful interference. It would also examine issues such as perimeter security, access control, the security of catering supplies and engineering services, passenger and baggage screening, reconciliation procedures, cargo security, surveillance mechanisms, lighting and the possible security threats posed to aircraft by cleaners, groomers and flight crews.⁸⁴

Wallis did not know if the IATA survey program continues today.⁸⁵

Transport Canada officials stated that many of Wallis's concerns were discussed during the development of the USAP, but that other perspectives were influential as well. Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the Commission hearings, expressed concern that having industry experts on audit teams might allow them to see sensitive commercial and state information.⁸⁶ He stated that ICAO built teams of auditors from a pool of very experienced aviation security professionals, some with extensive

82 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4720.

83 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4721.

84 Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4727-4732.

85 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4732.

86 Testimony of Jim Marriott, vol. 39, June 4, 2007, pp. 4732-4733.

industry experience.⁸⁷ Wallis countered that the possibility that industry experts might see sensitive information had never caused concern in the IATA survey program. He argued that airlines needed to be aware of sensitive security information to put appropriate security procedures in place. He testified about his concern that, under the USAP, using foreign government representatives as auditors might give them access to sensitive information about other states.⁸⁸ Wallis had earlier written that this was one of the concerns raised by states when the audit program was first proposed in 1989, and which led to the shelving of the concept at the time.⁸⁹

Marriott noted that the eight key survey activities that formed part of IATA's Intensified Aviation Security Program bore a "striking resemblance" to those carried out by USAP teams.⁹⁰ Marriott agreed that providing notice to states might permit them to improve their operations in advance of the audit, or come up with explanations or justifications. However, the time frame was normally only a few months. Marriott stated that this would not be enough time to implement significant enhancements. He explained that notice was necessary because of the amount of preparatory work required by the audit teams. The notice period allowed states to provide the team with documentation so it could study the state's regulatory instruments and structure, which in turn enabled an informed and comprehensive audit.⁹¹

Wallis raised concerns about the USAP, notably the potential for problems when a country conducts its own security audits. Extensive experience in aviation security at the ground level becomes all the more important for audit team members. Wallis offered a workable solution for the concerns he raised. He noted that ICAO and IATA, as organizations, were conceived at the same Conference on International Civil Aviation, held in Chicago in 1944,⁹² and that there has been an ongoing requirement for the two to collaborate.⁹³ A blending of their respective areas of expertise would provide the best solution, with civil servants and industry experts working together. In addition, those countries with the greatest expertise in monitoring aviation security standards, including Canada, should serve as the primary source of government expertise:

Continental governments that with their national air carriers have regularly participated in monitoring security standards around the world may be able to provide a nucleus around which ICAO can build. Canada, Australia, Singapore, and Japan may also make valid input. A combination of personnel from such governments plus aviation industry professionals, who have more than a passing interest in the standard of security

⁸⁷ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4733.

⁸⁸ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4739-4740.

⁸⁹ Wallis, *How Safe Are Our Skies?*, p. 72.

⁹⁰ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4734.

⁹¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, pp. 4724-4725.

⁹² Wallis, *Combating Air Terrorism*, p. 91.

⁹³ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4723.

at international airports, could be the way ahead. In any event, ICAO officials will have to bite on one unpalatable bullet: They must accept that most of their contracting states will not have the expertise to participate as team players in any audit program. Such states will instead need to be recipients of the service.⁹⁴

Wallis warned of the inherent difficulties of working within international fora. He noted the remarks of Dr. Assad Kotaite, a former ICAO Council President, following the decision to develop an international audit program: "...This is a historic moment in the evolution of civil aviation. I am extremely proud of the work we have achieved at this Conference and I am convinced that it will contribute greatly to protecting lives, restoring public confidence in air travel, and promoting the health of air transport."⁹⁵ Wallis said that such rhetoric, or "glorified language,"⁹⁶ within the international community must not be allowed to mask the need for real change in aviation security. Rules, programs and policies may be put into place, but it is their application that matters:

I'm not sure that any announcement actually strengthens international aviation security. It comes down to application of the intentions behind such an announcement.

I am always suspicious when the rhetoric rises...and often new announcements are sort of sound bites which have some sort of political value. But it comes down to what actually is implemented.⁹⁷

Wallis testified about his continuing worry about the state of aviation security around the world and was "...yet to be convinced that the international response to 9/11 is quite the response that we need."⁹⁸ Still, he acknowledged the important role of ICAO:

And really, having an opportunity for states to come together to debate and discuss the situation is very valuable. And that to me is the real value of ICAO. It provides a chamber in which the...contracting states of the organization can discuss security matters. It is there that I personally would look not for rhetoric but for input by the major states who can be an influence on the smaller ones, even to the extent of funding certain things in a smaller state either by way of aid or simply as a bilateral relating to civil aviation operations.⁹⁹

⁹⁴ Wallis, *How Safe Are Our Skies?*, pp. 73-74.

⁹⁵ Wallis, *How Safe Are Our Skies?*, p. 74.

⁹⁶ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4722.

⁹⁷ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4747.

⁹⁸ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4722.

⁹⁹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4748.

3.1.2.3 North America

The US reacted quickly to the September 11th attacks, passing legislation in November 2001 that transferred federal responsibility for passenger and baggage screening from the Federal Aviation Administration (FAA) to the Transportation Security Administration (TSA), which later became part of the Department of Homeland Security (DHS). The new legislation required that all checked baggage be screened and that screeners be certified.¹⁰⁰

With the threat presented by September 11th – that of suicide attackers commandeering aircraft for use as weapons¹⁰¹ – the United States decided it would no longer permit aircraft to land at Ronald Reagan Washington National Airport (Reagan National Airport)¹⁰² without an air marshal on board.¹⁰³ The main concern was the proximity of the airport to significant government landmarks in Washington.¹⁰⁴ The US asked Canada to deploy only RCMP officers as air marshals travelling to Reagan National Airport. Transport Canada then directed the RCMP to develop an air marshal program to enable Canadian flights to land at Reagan.¹⁰⁵ The Canadian Air Carrier Protective Program (CACPP) was implemented in 2001.¹⁰⁶

On December 12, 2001, Canada and the US signed the Smart Border Declaration, with its 30-point Action Plan designed to enhance the security of their shared border while facilitating legitimate flows of people and goods. The Declaration included measures related to aviation security, such as the development of common standards for biometric identifiers on travel documents,¹⁰⁷ the mutual recognition of national security standards and the sharing and analyzing of transborder and international passenger information.¹⁰⁸

Since June 2005, the United States, Canada and Mexico have co-operated to protect aviation in North America from terrorist threats.¹⁰⁹ A joint statement issued on March 31, 2006 declared that innovative risk-based approaches to improving security and facilitating trade and travel would be encouraged. These were to include close coordination on infrastructure investments and vulnerability assessments, screening and processing of travellers, baggage and cargo, a single integrated North American trusted traveller program and swift law enforcement responses to criminal or terrorist threats.¹¹⁰

¹⁰⁰ Exhibit P-157, p. 96 of 135.

¹⁰¹ Exhibit P-157, p. 93 of 135.

¹⁰² The Ronald Reagan Washington National Airport is also referred to by the code “DCA.” See Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8059-8060.

¹⁰³ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8059.

¹⁰⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8060.

¹⁰⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8059-8060.

¹⁰⁶ Exhibit P-157, pp. 105-106 of 135.

¹⁰⁷ The NEXUS Air program uses biometric recognition technology to identify pre-approved, low-risk Canadian and US travelers for facilitated entry through Customs and Immigration to both countries. See Exhibit P-157, p. 96 of 135.

¹⁰⁸ Exhibit P-157, p. 96 of 135.

¹⁰⁹ Exhibit P-157, p. 96 of 135.

¹¹⁰ Exhibit P-157, p. 96 of 135.

3.1.2.4 Europe

Before September 11, 2001, there was no binding mechanism in Europe to ensure the proper application of security standards outlined by ICAO and the European Civil Aviation Conference (ECAC), an intergovernmental organization established to promote a safe, efficient and sustainable European air transport system. To remedy this, the European Union (EU) introduced a security policy to give legal force to the rules and mechanisms for co-operation at the EU level.¹¹¹ On January 19, 2003, a mandatory European Council Regulation (2320/2002) came into effect, establishing security standards at all EU airports.¹¹² Under the regulation, National Aviation Security Programmes and National Quality Control Programmes were established to ensure proper implementation of security standards. The EU also acquired the authority to inspect the security procedures of all member airports and to demand compliance with the new rules.¹¹³ The Annex to the regulation, as well as its implementing regulations, contained detailed rules for improvements in many areas: airport security, including access control and 100 per cent staff screening; aircraft security, including aircraft inspections and protection of the aircraft when in and out of service; passenger and cabin baggage screening; hold baggage screening and protection (positive passenger-baggage reconciliation had been mandatory in most European countries since 1989); cargo, courier and express parcels, including detailed rules on the handling, screening and protection of cargo; company mail and materials and public mail; air carrier catering, cleaning, stores and supplies; general aviation; staff recruitment and training; and equipment standards.¹¹⁴

3.1.3 Canadian Response

3.1.3.1 Introduction

As noted earlier, the attacks of September 11th resulted in a major transformation of Canada's civil aviation security regime. According to the CATSA Advisory Panel, the Government of Canada made it an urgent priority to enhance the country's counterterrorism capabilities and preparedness. This effort included a renewed focus on aviation security.¹¹⁵

As the September 11th attacks were unfolding, rapid decisions were made about North American aviation security. The result was an "...unprecedented shutdown of the aviation system in North America."¹¹⁶ Canada acted as a haven for aircraft that required redirection to safe locations. The Government of Canada worked closely with the FAA to divert aircraft, all the while aware that some of these aircraft might also risk being hijacked. Aircraft were met by police and customs officials.

¹¹¹ Exhibit P-157, pp. 96-97 of 135.

¹¹² Exhibit P-157, p. 96 of 135.

¹¹³ Exhibit P-157, p. 97 of 135.

¹¹⁴ Exhibit P-157, p. 97 of 135.

¹¹⁵ Exhibit P-169, p. 16 of 202.

¹¹⁶ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4534.

One of the most difficult steps afterwards was restarting “the whole system.”¹¹⁷ Initial security enhancements addressed areas that were considered to be highest risk, including the pre-board screening (PBS) of passengers and their carry-on baggage, the enhancement of security on board aircraft, and airport control.¹¹⁸ Airports received very clear directions to supplement their access control systems with security personnel at doors.¹¹⁹ Police presence was increased at airports and directions were issued to lock the cockpit doors of passenger aircraft departing from Canadian airports.¹²⁰ Increased monitoring by aviation security inspectors was another measure.¹²¹ The Government of Canada also assumed third-party war risk liability following the withdrawal of insurance from the commercial sector, so that the aviation industry could continue operating.¹²²

The Government’s response had yet another dimension. Jean Barrette, Director of Security for Transport Canada, testified that significant efforts were made after September 11th to ensure that the Canadian public was adequately informed that air terrorism could hit close to home:

...[P]ost-9/11 saw a very, very wide range of awareness material, again, going down to the public creating that awareness that perhaps Canada could no longer enjoy what I called the ‘Canadian naivety’ around security; that terrorism was not only something happening on the other side of the ocean but that following the attack on the towers in New York, that it was very, very close to home.¹²³

In October 2001, the Government announced increased funding initiatives for security:

- More than \$79 million for new equipment and supporting activities at airports;
- \$55.7 million for the purchase and deployment of advanced explosives detection systems (EDS), which had been in development, and which the Government now pressed to be developed more rapidly;
- Funding for 28 additional airport security inspectors; and
- Training programs for cargo and baggage handlers and airline and airport staff to support implementing the new technologies.

117 Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4534.

118 Exhibit P-157, p. 97 of 135.

119 Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4535.

120 Exhibit P-157, p. 97 of 135.

121 Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4535.

122 Exhibit P-157, p. 97 of 135.

123 Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4843.

Transport Canada also published enhanced security requirements for air carriers and airport operators. These included screening for electrical and electronic devices and sharp and other dangerous objects in carry-on baggage, cockpit protection and protection of US-bound aircraft.¹²⁴ Besides the obligatory presence of armed police officers on flights to Reagan National Airport, Canada made other adjustments to its aviation security regime to accommodate special US requirements for these flights, including additional advance passenger information (API) and extra security requirements for the preparation and take-off of aircraft.¹²⁵

A second wave of aviation security initiatives was identified in the December 2001 federal Budget "...[a]s the full impact of the events of September 11, 2001, was realized."¹²⁶ Barrette described the significance of the funding provided in the Budget:

[The] December 2001 budget announcement by the Government was...an unprecedented investment in aviation security in Canada. This resulted in an investment in security of over \$2.2 billion.... [T]his is significant for Canada. That resulted in basically a five-year plan in increasing capacity. Thirty-five million dollars were invested in reinforcing cockpit doors of commercial aircraft, increased policing at airports and a very, very important element was also the creation of [the] Canadian Air Transport Security Authority, which came into being in April 2002.¹²⁷

In April 2002, the Canadian Air Transport Security Authority (CATSA) was created as a Crown Corporation by the *Canadian Air Transport Security Authority Act (CATSA Act)*.¹²⁸ CATSA assumed several core security functions, particularly the screening of passengers, carry-on baggage and checked baggage. Unlike the Government's response following the loss of Air India Flight 182, the response to the events of September 11th saw responsibility for screening transferred from air carriers to a government entity. The CATSA Advisory Panel concluded that leaving the screening of passengers and baggage to the air carriers after the Air India bombings was a serious weakness in the security system, since security would not be the carriers' primary concern.¹²⁹ Even the bombing of Pan Am Flight 103, which flowed from the same security weakness, did not prompt such change. It was only after September 11th that the recommendations of the 1985 Seaborn Report, commissioned by the Government of Canada to review aviation security, were taken further.¹³⁰

¹²⁴ Exhibit P-157, p. 98 of 135.

¹²⁵ Exhibit P-157, p. 98 of 135.

¹²⁶ Exhibit P-157, p. 98 of 135.

¹²⁷ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4536.

¹²⁸ S.C. 2002, c. 9, s. 2, s. 5(1); see also Exhibit P-169, p. 16 of 202.

¹²⁹ Exhibit P-157, p. 67 of 135.

¹³⁰ Exhibit P-157, p. 98 of 135.

Marriott, in his testimony before the Commission, acknowledged the benefits of having a single government organization responsible for the security of passengers and baggage. He noted that, when screening was left to the air carriers, it was administered in a less coordinated fashion nationally. With CATSA, a single set of standard operating procedures governed screening personnel across the country, and more uniform training was provided to them.¹³¹

In November 2002, CATSA's role was expanded to include the random screening of non-passengers who sought access to restricted areas of airports.¹³² At the same time, CATSA was assigned responsibility for developing and implementing the Restricted Area Identification Card (RAIC) program. The program was designed to augment the existing security access control system, which required all non-passengers to carry a Restricted Area Pass (RAP) to enter restricted areas. The RAIC program incorporated into the RAP biometric identifiers that were linked to a central database and that permitted the tracking of cardholders.¹³³ The December 2001 Budget funded other security initiatives, some of which echoed the enhancements highlighted in the October 2001 funding announcement:

- The hiring of 59 additional Transport Canada security inspectors;
- Up to \$30 million for aircraft security modifications, including reinforced cockpit doors;
- \$1 billion over five years for the purchase of EDS for baggage screening;
- Increased police presence and security at airports; and
- A program of armed RCMP officers ("air marshals") on aircraft.¹³⁴

The Budget also introduced new limits for carry-on baggage, as well as random secondary searches of passengers for flights to the US.¹³⁵ The Budget created the Air Travellers Security Charge (ATSC), a fee to be paid by travellers beginning April 1, 2002. The revenues were to help fund many new aviation security initiatives, including CATSA.¹³⁶

Also in reaction to the September 11th attacks, Parliament enacted the *Public Safety Act, 2002*.¹³⁷ Under the Act, which came into force in stages, beginning

¹³¹ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4538.

¹³² A non-passenger is anyone who works at an airport, who visits an airport to provide services or deliver goods or who requires access to an airport's restricted areas. Screening is similar to passenger screening. See Exhibit P-169, p. 18 of 202.

¹³³ Exhibit P-169, p. 18 of 202.

¹³⁴ Exhibit P-157, p. 99 of 135.

¹³⁵ Exhibit P-157, p. 99 of 135.

¹³⁶ There has been criticism that the revenues from the ATSC are collected and disbursed in a non-transparent manner, making it difficult to confirm that the funds are indeed spent on aviation security initiatives. Changes have been called for by a number of stakeholders. See Exhibit P-169, pp. 168-169 of 202; see also Section 3.10, which discusses the concerns surrounding the ATSC in greater detail.

¹³⁷ S.C. 2004, c. 15.

in May 2004, certain departments and agencies received authority to collect passenger information for transportation and national security purposes. Interim orders could also be issued in emergencies, and provisions were included to deter the proliferation of biological weapons and to provide greater control over explosives and hazardous substances.¹³⁸ The Act also significantly amended the security provisions of the *Aeronautics Act*. The Minister of Transport received explicit authority to introduce confidential security measures, to grant, suspend or cancel security clearances for Restricted Area Passes, and to delegate authority to give emergency directions in the face of immediate threats to security. Offences were created for persons endangering the safety or security of aircraft or persons on board.¹³⁹

The *Public Safety Act*, 2002 gave Transport Canada the authority to identify individuals who were threats to aviation security and led to the establishment of Canada's first "no-fly" list, known as the Passenger Protect Program.¹⁴⁰ Development of the Program began in 2004¹⁴¹ and it came into effect on June 18, 2007.¹⁴² The Program involved creating a list of individuals who might pose an immediate threat to aviation security if they boarded a flight.¹⁴³ Transport Canada could require airlines to provide information about such individuals¹⁴⁴ and to issue Emergency Directions if an immediate threat to security was perceived.¹⁴⁵ The Program is now used as an additional pre-board passenger screening tool.

The *Public Safety Act*, 2002 also amended the *Aeronautics Act* to address the security of foreign aircraft arriving in Canada. Transport Canada was given authority to conduct security assessments of air carriers and facilities outside Canada. The Foreign Security Inspection Program became responsible for conducting assessments of foreign air carriers and airports to ensure that Canadian security requirements for flights destined for Canada were implemented. If security concerns arose, periodic and random inspections could be conducted.¹⁴⁶

Following the September 11th attacks, training was enhanced for Transport Canada inspectors and for air carrier passenger service agents. In 2002, for example, briefing sessions that provided an overview of the changes to security measures since September 11th were given across Canada to passenger service agents working at airports. In 2003, Transport Canada established a working group to address training requirements for ground personnel and revised its cargo screening training program for all employees engaged in accepting cargo for transport on passenger aircraft. In the summer of 2004, a national air cargo security awareness campaign began.¹⁴⁷

¹³⁸ Exhibit P-157, p. 99 of 135.

¹³⁹ Exhibit P-157, p. 100 of 135.

¹⁴⁰ Exhibit P-157, p. 100 of 135; see also Section 3.5.3.2.1, which discusses the Passenger Protect Program in detail.

¹⁴¹ Exhibit P-157, p. 100 of 135.

¹⁴² Exhibit P-278, Tab 8, p. 1.

¹⁴³ Exhibit P-157, p. 100 of 135.

¹⁴⁴ Exhibit P-157, p. 100 of 135.

¹⁴⁵ Exhibit P-278, Tab 13, p. 8.

¹⁴⁶ Exhibit P-157, p. 100 of 135.

¹⁴⁷ Exhibit P-157, p. 101 of 135.

The events of September 11th have continued to influence aviation security in Canada. In 2005, Transport Canada began to develop a national Transportation Security Action Plan for security programs in all transportation modes. The Plan's goal was to assess current and future threats to transportation, evaluate what had already been achieved and identify future challenges and priorities, using a risk management model.¹⁴⁸ The Plan was expected to serve as a road map for security programs in all modes of transportation for the following five to seven years.¹⁴⁹

The 2006 Budget provided new funding of \$133 million over two years to assist CATSA with increased costs due to the growth in air traffic. The funding would support CATSA's security services, including passenger and baggage screening. The Budget also committed up to \$26 million over two years for improving air cargo security. In August 2006, Canada participated in a multi-country coordinated response to the threat uncovered in the UK involving liquids and gels. Canada updated its list of prohibited items for carry-on baggage and permitted only small quantities of liquids, gels and aerosols to be carried on passenger flights.¹⁵⁰

The 2008 Budget took into account that significant operational pressures and continued growth in air traffic would challenge CATSA's ability to handle its future screening responsibilities. Acknowledging the ongoing risk that terrorists posed to civil aviation, the Budget pledged \$147 million to assist CATSA.¹⁵¹

In January 2009, the Government of Canada announced additional funds to support passenger, baggage and cargo security. The 2009 Budget stated that "...[n]ew and enhanced aviation security measures are required to strengthen the security of Canadians; ensure that Canada remains closely aligned with the security measures of its key international partners; and ensure that Canadian airports and air carriers remain competitive internationally."¹⁵² It promised \$282 million over the following two years to support the development of aviation security plans, improve CATSA operations and implement a new passenger assessment system. The measures included new, advanced screening equipment and other technology and improved training for screening personnel. The 2009 Budget also promised \$14 million in 2009-2010 to help implement a new air cargo security program at Canadian airports.¹⁵³

3.1.3.2 Canadian Air Carrier Protective Program

The Canadian Air Carrier Protective Program (CACPP) is an air marshal program that deploys specially trained RCMP officers, known as Aircraft Protective Officers (APOs), to provide covert, armed security in the airport environment and on aircraft.¹⁵⁴

¹⁴⁸ Exhibit P-157, p. 101 of 135.

¹⁴⁹ Exhibit P-263, Tab 23, p. 2 of 2.

¹⁵⁰ Exhibit P-157, p. 101 of 135.

¹⁵¹ See Exhibit P-465.

¹⁵² See Exhibit P-407.

¹⁵³ See Exhibit P-407.

¹⁵⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8073.

3.1.3.2.1 *Genesis and Development of the CACPP*

Although long established in the US, air marshal programs came relatively recently to Canadian aviation. The programs were introduced in the United States in the 1970s¹⁵⁵ in response to a series of domestic and foreign hijackings. The objective was to use what were then termed “sky marshals” to protect against hijackings.¹⁵⁶

As noted, after September 11th, the threat of suicide attackers using aircraft as weapons led the US to deny aircraft permission to land at Reagan National Airport without an air marshal on board.¹⁵⁷

The CACPP was implemented in 2001, and was originally funded by CATSA through federal appropriations.¹⁵⁸ The sole focus of the CACPP initially was to provide APO coverage for all flights to Reagan National Airport. The program later evolved to provide APOs on selected Canadian commercial aircraft¹⁵⁹ flying to certain destinations.¹⁶⁰ As the program grew and became better funded, it was able to assume additional tasks. The CACPP received requests for APO assistance in other locations where threats appeared to warrant this measure. The CACPP started to design protocols for particular destinations to which APOs were flying on a regular basis. While APOs at first flew to these locations due to specific circumstances, a more regular pattern of deployment was established with the development of a “threat matrix.”¹⁶¹

3.1.3.2.2 *Threat Matrix*

About two years after the CACPP began, a threat matrix was created to provide a consistent method for determining routine and more urgent APO deployments.¹⁶² The matrix is an internationally-accepted tool that has been studied and tested throughout the world.¹⁶³ It was developed by the Civil Aviation Protective Intelligence (CAPI) Unit of the RCMP. The CAPI Unit is directly connected to the APO program.¹⁶⁴

The threat matrix grades flights according to specific factors, such as destination. Because resources are limited, the matrix identifies flights with the highest

¹⁵⁵ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7985. See also Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4212; Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4982; Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8058.

¹⁵⁶ Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4211- 4212.

¹⁵⁷ Exhibit P-157, p. 93 of 135; Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8059.

¹⁵⁸ Exhibit P-157, pp. 105-106 of 135. Funding arrangements were altered as of April 1, 2008. Funding is now provided directly to the Royal Canadian Mounted Police (RCMP), as discussed below. See Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8075.

¹⁵⁹ See Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8100; see also Exhibit P-157, p. 110 of 135.

¹⁶⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8060.

¹⁶¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8060.

¹⁶² Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8066, 8076.

¹⁶³ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8076.

¹⁶⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8066.

potential for an incident. The matrix also determines which domestic and international flights require APOs on an ongoing basis, within the confines of the resources available.¹⁶⁵

The threat matrix determines the routine scheduling of APOs on various flights and is also influenced by explicit threats against particular aircraft and global events on a given day.¹⁶⁶ The CAPI Unit provides threat assessments, for example, on events in particular cities to which Canadian aircraft fly. The information is fed into the matrix¹⁶⁷ and routine flight schedules for APOs may be altered accordingly.¹⁶⁸

RCMP Superintendent Alphonse MacNeil testified that he would “highly doubt” that an aircraft facing a very specific threat would fly until the threat was thoroughly investigated and cleared.¹⁶⁹ In other words, with a very specific threat, it would be highly unlikely that the security response would be simply to place an APO on board and allow the aircraft to fly.

3.1.3.2.3 Role of Aircraft Protective Officers

Although the term “air marshal” is commonly used, ICAO uses the term “in-flight security officer,”¹⁷⁰ which is now considered the generic description.¹⁷¹ Other countries with air marshal programs may use different terms. Australia, for example, uses the term “aircraft security officers.”¹⁷²

Other countries often require their air marshals to perform additional duties, such as protective policing. Canada’s Aircraft Protective Officers (APOs), on the other hand, must commit their time fully to their duties as APOs.¹⁷³ APOs are trained, armed officers who conduct covert operations.¹⁷⁴ Their responsibilities are not limited to in-flight security, but also extend to security in the airport environment.¹⁷⁵ Besides preventing the commandeering of aircraft, APOs remain vigilant for other terrorist activity and assist in controlling criminal activity. In doing this, APOs both gather and use intelligence. They are trained to use observational skills, including behavioural analysis techniques, and to intervene only in extreme circumstances. APOs are most effective when their identities remain unknown to passengers and when their activities are covert.

The Commission was told that the value of air marshal programs, in large part, was their deterrent effect.¹⁷⁶ While APOs were not placed on all flights, apart

¹⁶⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8066, 8076.

¹⁶⁶ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8066, 8076.

¹⁶⁷ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8075-8076.

¹⁶⁸ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8066, 8076.

¹⁶⁹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8067.

¹⁷⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8059.

¹⁷¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4768.

¹⁷² Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8059.

¹⁷³ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8067.

¹⁷⁴ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4768.

¹⁷⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8073.

¹⁷⁶ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7985.

from those to Reagan National Airport, the program served as a deterrent because they could be present on any flight.¹⁷⁷

MacNeil testified that there had been no incidents to that point of “having to take someone down on an aircraft.”¹⁷⁸ This could have been due in part to the deterrent effect of the program, according to Captain Craig Hall, Director of the National Security Committee of the Air Line Pilots Association, International (ALPA):

...We get back to the randomness; people are a little bit more reticent to do something bad to an aircraft if they think they may run into a marshal's team....

So I think as I said, a very large measure of success is the fact that I think that there's a very, very big deterrent value. I don't think you can really quantify the success any further than that because it is hard to quantify a negative result, but in security that's a lot of what we do.¹⁷⁹

The Commission questioned the deterrent effect, however, because publicity about the APO program appeared to be minimal. Dr. Reg Whitaker, Chair of the CATSA Advisory Panel, agreed that, although this information had been in the public domain for some time, the general public might need to be better informed that an air marshal might be on board any Canadian-registered airline. This information could be provided in a way that does not jeopardize national security or alert terrorists about how the program operates.¹⁸⁰ MacNeil agreed that there was a need for greater public awareness about the program and the work of APOs on aircraft and in airports. The CACPP is currently working on methods to better inform the public. MacNeil stated that testimony before the Commission might have served as one means to increase public awareness.¹⁸¹

In-Flight Security

When an APO is to be placed on an aircraft, the CACPP informs the air carrier. It is the carrier's responsibility to inform the pilot-in-command and chief flight attendant of the APO's presence and seat location.¹⁸²

If an attempt is made to commandeer an aircraft, the APO is capable of intervening empty-handed or with a firearm.¹⁸³ The Canadian program sets

¹⁷⁷ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5282.

¹⁷⁸ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8072. See also Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7985.

¹⁷⁹ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 7985-7986.

¹⁸⁰ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4602-4603.

¹⁸¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8072, 8088.

¹⁸² Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8080-8081,

¹⁸³ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8079.

clear guidelines about the timing and method of intervention.¹⁸⁴ The threshold is high. APOs intervene only where the integrity of the aircraft is at risk or where there is a serious risk of harm to an individual. Until then, APOs must maintain their cover.¹⁸⁵ The key to success is the element of surprise, which gives an important advantage to an APO when attempting to overpower an individual intent on committing a violent act.¹⁸⁶

The disruption caused by an unruly passenger, for example, would not meet the threshold for intervention.¹⁸⁷ Flight crews are well-trained to handle such passengers and do so when APOs are not on board.¹⁸⁸ The CACPP is aware that one tactic to identify an APO on an aircraft is for a “passenger” to create a disturbance.¹⁸⁹

Airport Security

APO responsibilities are not limited to in-flight security. They also provide armed, covert security in the airport environment.¹⁹⁰ Areas outside the secured zones of the airport terminal are considered potential targets. Congestion caused by long queues at airline check-in and security screening counters creates a “target-rich” environment because many people are gathered in a confined area. Similarly, during security breaches, passengers are routinely evacuated from secure areas, causing congestion in non-secure areas of the airport terminal.¹⁹¹ An attack in July 2007 on a non-secure area of Glasgow Airport, using a vehicle loaded with propane canisters, illustrated the vulnerability of such areas.¹⁹²

Recognizing the growing security concerns surrounding the airport environment, the CACPP training program is evolving to provide greater emphasis on these concerns, including problems associated with crowds and security at the boarding gate.¹⁹³

¹⁸⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8097.

¹⁸⁵ The approach to intervention is not graduated; there is one, high-level threshold which must be met before an APO will engage in an interventional activity. See Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8079. See also Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8098.

¹⁸⁶ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8078.

¹⁸⁷ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8097.

¹⁸⁸ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8099.

¹⁸⁹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8098.

¹⁹⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8073.

¹⁹¹ The CATSA Advisory Panel suggested that “[...]olutions to this situation of vulnerability could be as drastic as redesigning a terminal building, or could involve integrating the security process into other layers, thereby reducing the number of passengers congregating in one location. Emergency evacuation procedures should also be reassessed by the appropriate authorities (the Airport Security Committees) to avoid the necessity of a crowd gathering in a small area”: Exhibit P-169, p. 57 of 202.

¹⁹² Canadian Broadcasting Corporation, “Britain remains on highest alert, 5 suspects arrested” (July 1, 2007), online: CBC <<http://www.cbc.ca/world/story/2007/07/01/glasgow-attack.html>> (accessed January 16, 2010). See also Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8073.

¹⁹³ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8074.

General APO surveillance also assists in identifying potential criminal activity at airports. In 2007, the Standing Senate Committee on National Security and Defence reported that organized crime was a serious concern at Canada's airports, with some organizations possibly linked to terrorist activities.¹⁹⁴ APOs are aware of the potential for criminal activity and, as trained observers, can help mitigate such activity.¹⁹⁵ MacNeil testified that APOs are trained and well-suited to recognize both terrorist and other criminal activity.¹⁹⁶

APOs generally do not become involved if they observe suspicious activity or behaviour, except in emergency situations. Instead, they notify the appropriate unit at the airport.¹⁹⁷

Behavioural Analysis

MacNeil confirmed that APOs use behavioural analysis techniques.¹⁹⁸ He stated that these techniques assess behavioural cues only and do not involve judgments based on racial, ethnic or cultural background. They are not based on dress or appearance.¹⁹⁹ Behavioural analysis gauges the reactions of individuals to changes in the environment, such as the arrival of a uniformed officer in the airport. Such an occurrence, for example, could cause concern for an individual with malicious intent, who might then exhibit particular behaviours that APOs are trained to detect.²⁰⁰

Training in these techniques includes promoting an awareness that individual reactions to environmental stimuli might differ because of cultural or racial background. MacNeil stated that it is impossible to provide instruction on the range of reactions from all cultures, but that "no one reaction will stand on its own":

... [O]ur people are trained not to look at one specific reaction and say, "Oh, I know what that means." It's a cumulative effect of a lot of reactions that we're looking for....²⁰¹

Many factors must be present before an individual's behaviour can be considered suspicious. MacNeil stated that training takes into account that many airports are international environments. He stated that a lack of awareness of cultural and racial differences would make APO operations ineffective.²⁰²

¹⁹⁴ Exhibit P-172, p. 17 of 155.

¹⁹⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8087.

¹⁹⁶ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8073.

¹⁹⁷ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8073, 8087-8088.

¹⁹⁸ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8075.

¹⁹⁹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8089.

²⁰⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8075.

²⁰¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8090.

²⁰² Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8090-8091.

Intelligence

Intelligence within the CACPP flows in two directions. The CACPP receives intelligence from the CAPI Unit, which in turn obtains its intelligence from the Integrated Threat Assessment Centre (ITAC),²⁰³ among other sources. APOs also generate intelligence in performing their duties and they give the RCMP information they acquire relating to national security and criminal intelligence.²⁰⁴ A tactical intelligence unit exists within the CACPP. A tactical intelligence officer positioned at each field unit receives information, for example, from the local Criminal Analysis or Organized Crime Investigation Section. The information is then shared with APOs. This might include information about the identity of a specific individual. APOs then act as “eyes and ears” in the airport and on aircraft, and can report any information obtained.²⁰⁵

MacNeil said that information obtained through the Passenger Protect Program, which maintains and manages Canada’s “no-fly” list, might be shared with the CACPP via the CAPI Unit. He testified that it is rare for the CACPP to receive information from the CAPI Unit about passengers in particular seats, but that such information would be shared with the CACPP if the CAPI Unit has it and if there is a threat.²⁰⁶

The CACPP shares information with its international partners about world trends and events. If the CACPP obtains information about a specific incident and other programs would benefit from the information, it will be shared. MacNeil stated that the CACPP adheres to all rules governing the sharing of specific information.²⁰⁷

3.1.3.2.4 Criticism of Air Marshal Programs

During Commission hearings, experts and industry stakeholders disagreed about the benefits of air marshal programs. Wallis, the Commission’s main expert on international aviation security, saw no value in the programs. He stated that “[t]here is no place for a weapon of any sort in the cabin of an airplane,” and that a firearm could be turned against the aircraft if it fell into the hands of a terrorist.²⁰⁸ He challenged the deterrent effect of such programs for several reasons. The presence of sky marshals in the 1970s had, at least once, failed to prevent a hijacking.²⁰⁹ On another occasion, a plane crashed because

²⁰³ The Integrated Threat Assessment Centre (ITAC) is a functional component of the Canadian Security Intelligence Service (CSIS). It is a community resource, staffed by representatives of a number of government departments and agencies, whose primary objective is to produce comprehensive terrorist threat assessments for timely distribution within the intelligence community. See Exhibit P-169, p. 33 of 202. See also Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8077.

²⁰⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8077.

²⁰⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8087.

²⁰⁶ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8085.

²⁰⁷ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8077.

²⁰⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 4765, 5009.

²⁰⁹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4766.

of a fight that occurred while the plane was airborne.²¹⁰ Wallis argued further that if terrorists were aware that APOs were on certain flights, such as those to Reagan National Airport, they will simply choose other flights. Wallis also argued that today's terrorists might be willing to perish for their cause, so that a shoot-out with an armed marshal would not cause them concern if they succeeded in their objective.²¹¹ As well, terrorists had operated in teams in recent years, so that a "small army" of air marshals would be required to defeat them. Wallis saw "only one outcome" of a fight in such circumstances.

Dr. Kathleen Sweet, another international aviation security expert, was also skeptical about the value of air marshals. She acknowledged that "any tool in the toolbox" was useful, but was concerned about the lack of training for air marshals – a particular problem in the United States, she said – as well as cost effectiveness.²¹² On both counts, improvements were necessary. Training was critical to ensure that APOs discharged their duties competently and with the appropriate authorization.²¹³ As well:

...[T]he key to airport security is on the ground, not once the plane is airborne. Once the plane is airborne, you have very limited resources to prevent something terrible from happening.²¹⁴

Options are limited once a flight is airborne, but this does not mean that legitimate security measures on board aircraft should be abandoned. Absolute security is not possible.²¹⁵ The Commission was repeatedly told about the benefits of a multi-layered approach to security; if one layer is by-passed, other layers remain.²¹⁶ The CATSA Advisory Panel identified the CACPP as one layer.²¹⁷ Any robust security regime must ensure that no gaps remain in the system.²¹⁸

The Standing Senate Committee on National Security and Defence (Senate Committee) concluded that locked cockpit doors on aircraft eliminated the need for air marshals,²¹⁹ but this position was challenged. Yves Duguay, Director of Security for Air Canada and a former RCMP officer, agreed generally with the CATSA Advisory Panel, stating that armed marshals represented one layer, possibly a significant layer, in a multi-layered approach:

210 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4767.

211 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4766.

212 Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4983.

213 Testimony of Jim Marriott, vol. 39, June 4, 2007, pp. 4768-4769.

214 Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4940.

215 Exhibit P-169, p. 36 of 202.

216 Exhibit P-169, p. 38 of 202.

217 Exhibit P-169, p. 39 of 202.

218 Exhibit P-361, Tab 1, p. 9.

219 Exhibit P-172, p. 52; see also Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4764.

The last barrier is the cockpit, the reinforced cockpit, and the one barrier before that would be the APO, the aircraft protection officer or the sky marshal of the United States.²²⁰

3.1.3.2.5 APO Recruitment, Training and Retention

Not all US air marshals are trained police officers. They come from various backgrounds and then receive special training. In Canada, all APOs are fully-trained RCMP officers.²²¹

Superintendent Greg Browning, Director of National and International Learning Services for the RCMP, had overall responsibility for APO training, recertification and training assets.²²² In describing the evolution of the APO training program, Browning suggested that it was probably "...one of the best programs that we have ever built from the ground up..." Duguay testified that he had visited the APO training centre and that he was impressed by the level of training. He saw the Canadian training program as "...probably one of the best programs."²²³

In its early days, the CACPP relied on the US air marshal training program. The Canadian program has evolved considerably since then and has been designed in consultation with international experts.²²⁴

APOs are carefully selected members of the RCMP.²²⁵ RCMP membership, which brings with it a recognized level of skills and training, is a prerequisite, but it alone is not sufficient. Applicants must demonstrate superior skills in several areas. Shooting skills, for example, must be better than the norm. As well, all applicants must pass specific psychological assessments and physical tests before admission.²²⁶

APOs undergo several weeks of basic training. They then proceed to their operational units. Recertification is required twice annually.²²⁷ Browning stated that Canada is the only country that requires recertification of its air marshals.²²⁸

In addition to the initial and recertification training courses, there is ongoing interaction between instructors and trainees. The National Training Centre is "hardwired" to the operational units, allowing for constant contact between instructors and the officers they train. The CACPP training program is unique in

²²⁰ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5282.

²²¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8058.

²²² Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8056.

²²³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5282.

²²⁴ Testimony of Greg Browning, vol. 65, October 24, 2007, pp. 8061, 8064.

²²⁵ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8061.

²²⁶ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8064.

²²⁷ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8061.

²²⁸ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8061.

that its instructors not only conduct training and recertification, but are required to fly as active APOs for a number of weeks each year.²²⁹

Training focuses on intervention skills, as well as observational and intelligence-gathering skills. These core skills are designed to enable APOs to interpret threats and behaviour, and to intervene only when absolutely necessary.²³⁰ Since they are active police officers, the roles of APOs are not limited to in-flight activities. According to Browning, their role begins when they start their day and continues during the drive to the airport, within the airport environment and while on the aircraft.²³¹ Training, in general, is focused on the strategies that individuals could use to hijack aircraft.²³²

Intervention training includes the use of the Incident Management/Intervention Model (IM/IM). This is a “use of force” model employed by police officers across Canada which dictates the intervention threshold in any scenario. APOs are required to use the IM/IM in deciding when and how to intervene.²³³ APOs receive training in personal intervention skills to deal with the entire spectrum of encounters from empty hand to firearms.²³⁴ The training facility also has aircraft fuselages to facilitate training.²³⁵

APOs are armed and their shooting skills must be of the highest standard. Browning stated that shooting skills standards for APOs are “...arguably the highest in the world.” He described the precision with which APOs use firearms as “surgical in nature.”²³⁶ Only RCMP members who have attained a certain score from the practical pistol course distinguishing them as marksmen are admitted. The APO training program further enhances their shooting skills through advanced courses and scenario-based drills.²³⁷

Browning stated that it is important for the entire operation to remain covert, from the identity of instructors and officers to their practices and training locations.²³⁸

APOs are recruited for three-year assignments. The RCMP places value in diversity, and its institutional policy requires members to acquire new skills and change positions regularly. A three-year limit was chosen because it was thought that this would benefit the organization and the members. Some APOs remain with the CACPP longer because they are promoted to supervisory positions.²³⁹

229 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8061.

230 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8062.

231 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8062.

232 Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8065.

233 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8064.

234 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8063.

235 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8063.

236 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8062.

237 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8063.

238 Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8063.

239 Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8080-8082.

MacNeil testified that most APOs report high job satisfaction and want to remain with the program beyond the three-year term.²⁴⁰

3.1.3.2.6 Flight Crew Training

The CACPP also trains pilots and chief flight attendants at its training centre. Specific scenarios are reviewed to prepare them for an intervention and to explain their roles and responsibilities. The CACPP is currently developing a tool to provide the same information without requiring attendance at the CACPP training centre. Airlines would use this in their ongoing training.²⁴¹

Hall spoke highly of the APO program and stated that the RCMP kept flight crews well-informed. He said that additional information on the expectations of “front-end” and “back-end” flight crew members during an incident would be welcomed.²⁴²

3.1.3.2.7 International Cooperation

Canada plays a leading role in the international air marshal community. MacNeil, on behalf of Canada's APO program, is Chair of the International Air Marshal Committee, which consists of representatives from the countries most active in delivering air marshal services.²⁴³ Representatives meet twice yearly in person and monthly via teleconference. According to MacNeil, these meetings provide an important forum for sharing information about issues around the world that affect air marshal programs.²⁴⁴

The Committee's main purpose is to share best practices.²⁴⁵ As an example, a request arose from a Committee meeting to develop specific scenarios involving hijackings. Ten scenarios were developed, each focusing on attempts to identify and eliminate the covert air marshal. Each scenario was analyzed and confirmed as a potential situation in which an individual could take over an aircraft. Mitigation strategies were then developed.²⁴⁶

Training scenarios and methodologies used in the program are not developed in isolation, but through co-operative international efforts. Besides sharing best practices at the International Air Marshal Committee, APO trainers discuss best practices and do case studies with other trainers from around the world. The CACPP's scenario-based training takes into account situations that have occurred or that might occur. Some of the CACPP's counterparts have experienced

²⁴⁰ The CACPP has conducted surveys to assess job satisfaction within the program. See Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8082.

²⁴¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8080-8081,

²⁴² Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7987.

²⁴³ MacNeil has been elected to two terms as Chair, commencing in September 2006. See Exhibit P-254.

²⁴⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8055.

²⁴⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8055.

²⁴⁶ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8065.

incidents, but not the CACPP. Browning stated that this might indicate the success of the Canadian program.²⁴⁷

3.1.3.2.8 Funding

The CACPP was initially funded by CATSA through federal appropriations.²⁴⁸ The *CATSA Act* allows CATSA to enter agreements with the RCMP for it to provide security services, including services on aircraft.²⁴⁹

In its 2006 review of the *CATSA Act*, the CATSA Advisory Panel recommended that CATSA be relieved of its responsibility for managing funding for the CACPP and that funding should be provided directly to the RCMP or through Transport Canada.²⁵⁰ MacNeil, who is responsible for financial issues pertaining to the program, told the Commission that, as of April 1, 2008, funding was to be provided directly to the RCMP.²⁵¹

The CATSA Advisory Panel observed that CATSA did not have any authority to direct or plan the CACPP²⁵² and that the program was not related to CATSA's core mandate.²⁵³ Reviews of the program were carried out periodically by an expert consultant. The Panel believed that a separate audit of the CACPP by the Auditor General or by an external auditor could serve just as well or better.²⁵⁴

3.1.3.2.9 Need for the Program

To date, there have been no incidents in Canada in which an APO has faced an attempted hijacking. MacNeil stated that the challenge faced by air marshal programs lies in the difficulty of showing the worth of the program when APOs are, it is hoped, never engaged.²⁵⁵ However, this dilemma is common to many who provide aviation security services, including those who conduct pre-board screening (PBS), hold bag screening (HBS) and non-passenger screening (NPS). Screeners, for example, must remain vigilant, despite the likelihood that most will never encounter a prohibited item such as a weapon.²⁵⁶

The APO program has been lauded by industry stakeholders as a world leader. The Commission acknowledges that the value of this program is impossible to assess, and it is likely that the deterrent value of air marshal programs will never be known. However, as long as Canadian commercial aircraft fly to Reagan National Airport and the United States continues to require the presence of air marshals, Canada will maintain its APO program. Using Canadian air marshals

²⁴⁷ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8074.

²⁴⁸ Exhibit P-157, p. 106 of 135.

²⁴⁹ *Canadian Air Transport Authority Act*, S.C. 2002, c. 9, s. 2, s. 28(2) [*CATSA Act*].

²⁵⁰ Exhibit P-169, pp. 70-71 of 202.

²⁵¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8075.

²⁵² Exhibit P-169, p. 70 of 202. See also Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4797.

²⁵³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4621.

²⁵⁴ Exhibit P-169, p. 70 of 202.

²⁵⁵ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8071.

²⁵⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4542.

under a Canadian program is far better than alternatives such as the imposition of foreign air marshal programs on Canadian aircraft or the development of a comparable security measure by the airline industry. In a system that depends on multi-layered security, this program may provide another layer to protect high-risk flights in the air and non-secure areas of airport environments, where protection is currently minimal.

3.1.4 After 9/11: Danger of Complacency Continues

The renewed focus on aviation security following the events of September 11th included closer, system-wide coordination between Canada and the United States.²⁵⁷ Many discussions focused on harmonizing the implementation of enhanced security measures.²⁵⁸ Marriott testified that such harmonization was merely the extension of a long-standing connection between the Canadian and US aviation regimes:

...Canada and the United States have always had a very close relationship on aviation security, and that's a matter of necessity because our aviation systems are so interlinked. We're each others largest aviation customer, if you put it that way.

A huge amount of traffic crosses the border daily. And we've had for many, many, many years a very close working relationship prior to 9/11 with the US Federal Aviation Administration and with its successor in the area of aviation security, the Transportation Security Administration, which sprang up after 9/11.

But it was apparent that, as close as our working relationship with the United States was, that relationship would need to be further intensified to best ensure that the security measures applicable to trans-border traffic were fully satisfactory at all times, and that we had a high level of operational readiness across the border.

So the frequency of contact with our US counterparts increased dramatically. Dedication of staff to manage that relationship increased incredibly immediately after 9/11 and our relationship has been ever stronger and ever growing since.²⁵⁹

Wallis had a different opinion of the security relationship between the two countries. He testified that the US conducted its civil aviation security affairs in

²⁵⁷ Exhibit P-157, p. 97 of 135.

²⁵⁸ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4535.

²⁵⁹ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4536-4537.

relative seclusion before September 11th. He had warned of the dangers of such an approach:

... I had warned sometime previously [before September 11, 2001], that whilst it was okay perhaps for the United States to be isolationist in its approach to aviation security, and that was based on their huge domestic operation that they had and which was why they wouldn't take on some of the international programs which we believed would have helped them, I did write and say that if the attitude of the terrorists changed and disposable or suicidal terrorists were to arise, then the earlier attitude of US security relating to aircraft is going to have to change. And we saw the suicidal terrorists in full flight, as it were, on 9/11.²⁶⁰

Wallis also stated that complacency could set in when the system did not experience an incident for a period of time, and that this could result in faltering government commitment to matters such as legislation to help promote security.²⁶¹

The Air India and Pan Am bombings focused world attention on aviation terrorism and on the need for strong security. Governments and other organizations subsequently worked together to enhance security measures around the world.²⁶² Even after these events, however, many of the measures that had been proposed by ICAO remained voluntary or were not adopted by Contracting States. By September 11th, few governments, including that of Canada, had introduced regulations to require the screening of all passengers and hold baggage on all flights. Few countries did positive passenger-baggage reconciliation. As well, despite the *Convention on the Marking of Plastic Explosives for the Purpose of Detection* (1991), which followed the bombing of Pan Am Flight 103, equipment at airports for detecting plastic explosives was relatively rare.²⁶³ As the CATSA Advisory Panel observed, the changes to global aviation security were incremental in the 15 years following the Air India bombing and the world was "shocked into a new era of accelerated reaction"²⁶⁴ after September 11th.

Despite the unparalleled commitment of Canada to enhancing civil aviation security following the September 11th attacks, critical gaps remain.²⁶⁵

3.1.5 Conclusion

A more careful examination of the history of unlawful interference against civil aviation and a greater observance of trends in terrorist activities might have

²⁶⁰ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4533.

²⁶¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4541.

²⁶² Exhibit P-157, p. 91 of 135.

²⁶³ Exhibit P-157, p. 91 of 135.

²⁶⁴ Exhibit P-157, p. 92 of 135.

²⁶⁵ Exhibit P-157, p. 104 of 135.

revealed the form that air terrorism was to take on September 11th. Like the bombing of Air India Flight 182, the 2001 attacks showed a failure of collective imagination in security matters.

Aviation security regimes around the world should have been more prepared than they were. Indeed, Wallis has argued that "...[t]here is very little that is new in threat or in aviation security generally. What is changing is the ability to respond."²⁶⁶

In most cases, the measures that were implemented after September 11th – such as strengthened passenger and baggage screening, improved oversight through inspections and audits, enhanced training for security personnel and the removal of core screening functions from air carriers – were merely the full realization of initiatives that were considered or should have been considered and implemented in response to the Air India and Pan Am bombings. Flaws in the system and the necessary corrective measures were well known. Nevertheless, it took a third major terrorism incident and the loss of thousands of lives before many of these measures were implemented.

3.2 Oversight in Aviation Security

Transport Canada is the designated authority ultimately responsible for national civil aviation security.²⁶⁷ However, operational responsibility for security measures is shared by a multitude of entities.²⁶⁸ Air carriers, airport operators, caterers, retail establishments at airports, ground-handling services, screening service providers and the Canadian Air Transport Security Authority (CATSA) are examples.²⁶⁹

²⁶⁶ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5009.

²⁶⁷ Under Standard 2.1.2 of Annex 17 to the *Chicago Convention on International Civil Aviation* ("Chicago Convention"), all Contracting States of the International Civil Aviation Organization (ICAO) are obliged to name a designated authority with responsibility for civil aviation security: "Each Contracting State shall establish an organization and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights." Transport Canada represents Canada at ICAO: Exhibit P-181, p. 2-1, s. 2.1.2; Exhibit P-169, p. 30 of 202; Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4271.

²⁶⁸ See, for example, Exhibit P-172, pp. 59-60 of 155, which provides a non-exhaustive list, prepared by the Standing Senate Committee on National Security and Defence, of organizations that have some responsibility for aviation security at Toronto Pearson International Airport.

²⁶⁹ Exhibit P-169, pp. 31-32 of 202.

These entities reflect a variety of organizational models, including private Sector.²⁷⁰ non-profit²⁷¹ and government.²⁷² For many, security is not their sole or necessarily even their primary concern. Security may be one of many priorities, or the need to pay attention to security may be merely a consequence of working in civil aviation.²⁷³ The physical environments in which these organizations operate also vary and can affect how security measures are implemented. Airports differ in size, layout, volume of traffic and types of security equipment available.²⁷⁴ Fixed Base Operations (FBOs) and the General Aviation (GA) sector have further differences,²⁷⁵ functioning outside the system of “designated” airports.²⁷⁶ As well, some industry participants may be obliged by Canadian programs or laws to carry out certain security operations at off-shore sites, beyond Canada’s physical borders, to be allowed to operate into Canada.²⁷⁷

Transport Canada must preside over these often substantially different entities. The Department is responsible for ensuring that each implements and adequately maintains civil aviation security measures in compliance with legislation and directives. This objective must be accomplished within a rather weak enforcement framework in which monetary or more severe penalties are rarely imposed and only as a last resort.²⁷⁸ In a system that relies heavily on voluntary compliance,²⁷⁹ the strength of Canada’s civil aviation security depends on vigilant oversight, a shared vision and absolute clarity in all communications.

Proper oversight of civil aviation security in Canada requires, in the first instance, a robust regulatory regime that prescribes a comprehensive set of security measures. Guidance – in the form of stipulated requirements – is found

²⁷⁰ Many retail establishments at airports, air carriers, independent screening contractors that provide screening officers to the Canadian Air Transport Security Authority (CATSA) and private aircraft and air services that form part of the General Aviation sector are some examples of entities that belong to the private sector. See Testimony of Georgina Graham, vol. 66, October 25, 2007, pp. 8232-8233; Exhibit P-169, p. 31 of 202; Exhibit P-101 CAF0827, pp. 2, 7 of 19.

²⁷¹ Airport authorities, for example, are incorporated as not-for-profit organizations. See Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8139.

²⁷² CATSA, for example, was established by the CATSA Act as a Crown Corporation on April 1, 2002. CATSA is responsible for several core security screening functions, including the screening of passengers and their baggage, as well as the screening of non-passengers and their belongings at major airports: Exhibit P-175, ss. 6(1); see also Exhibit P-169, pp. 16, 18 of 202.

²⁷³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5203.

²⁷⁴ Exhibit P-169, pp. 96, 103 of 202.

²⁷⁵ Exhibit P-169, p. 55 of 202.

²⁷⁶ In Canada, 89 airports have been designated to receive CATSA’s screening services, which represents approximately 99 per cent of all passenger traffic. Of the 89 airports, nine have been designated as Class 1, or major, airports, 20 are designated as Class 2, or intermediate, airports, and 60 are designated as Class Other, or smaller, airports. See Exhibit P-169, pp. 103, 199 of 202.

²⁷⁷ The Passenger Protect Program, Canada’s no-fly list, must be administered by air carriers whose flights will arrive at designated aerodromes in Canada. This may require administration of the Program outside of Canada’s borders for international flights arriving in Canada. See Exhibit P-278, Tab 13, p. 4.

²⁷⁸ See, for example, Exhibit P-101 CAF0827, p. 19 of 19.

²⁷⁹ The system of voluntary compliance represents a philosophy that originated in the post-1985 period and has continued today. See Exhibit P-263, Tab 15, p. 3 of 5 and Tab 20, p. 1 of 1.

at the international level. Annex 17,²⁸⁰ the security annex to the *Convention on International Civil Aviation* (“*Chicago Convention*”),²⁸¹ outlines the minimum security standards that must be applied by all signatories.²⁸² Most countries, including Canada, are signatories.²⁸³ As one of the wealthiest nations in the world, Canada should be able to exceed these standards, as all developed nations are encouraged to do.²⁸⁴

All aspects of Canada’s civil aviation security regime must address the prevailing threat environment appropriately.²⁸⁵ The system must be devised so that it both routinely accounts for all significant risks and it includes a carefully considered plan for responding to emergencies. Because civil aviation security presents a dynamic environment of risk,²⁸⁶ oversight must include the capacity to monitor the overall system constantly to ensure that it remains capable of thwarting terrorist threats and that the system can adapt quickly to changes in threats. This involves understanding past, present and future threats, including threats that arise in other parts of the world.

There are several key elements to an adequate regime: a solid understanding of the history of global air terrorism and its trends and patterns; a consistently proactive approach; a system of organized and intentional redundancy in which multiple, reinforcing layers of security are established;²⁸⁷ a flexible and performance-based approach;²⁸⁸ and the systematic application of commonly accepted risk management protocols.²⁸⁹

Oversight in civil aviation security must take into account that air terrorism threats transcend borders. Canada depends for its own security on the soundness of civil aviation security regimes established by other countries.²⁹⁰ Security weaknesses in one country can permit aircraft in that country to be used as an entry point for terrorists, possibly allowing them to bypass more stringent

²⁸⁰ The Eighth Edition of Annex 17 (April 2006) is the current edition. See Exhibit P-181.

²⁸¹ The 1944 *Chicago Convention* is the foundational treaty for international governance in civil aviation. See Exhibit P-150.

²⁸² There is an opt-out provision, however. Article 38 of the *Chicago Convention* enables Contracting States to notify ICAO of any differences between their national regulations and practices and the international standards contained in Annex 17, should they find it “impracticable to comply in all respects” or if it is deemed “necessary to adopt regulations or practices differing in any respect from those established by an international standard.” See Exhibit P-150, pp. 44-46, Art. 38. See also Exhibit P-181, p. (v); Testimony of Rodney Wallis, vol. 36, May 30, 2007, pp. 4270-4271.

²⁸³ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4270.

²⁸⁴ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4218.

²⁸⁵ Exhibit P-169, p. 26 of 202.

²⁸⁶ Exhibit P-361.

²⁸⁷ Exhibit P-169, p. 38 of 202.

²⁸⁸ Exhibit P-169, pp. 92-93 of 202.

²⁸⁹ Exhibit P-361, Tab 1, p.10.

²⁹⁰ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4746.

controls elsewhere.²⁹¹ Besides monitoring the global aviation security situation for its impact on Canada, Transport Canada's oversight responsibilities should include offering support and leadership to strengthen civil aviation security around the world.

Although Canada has made substantial progress in many areas of security since the bombing of Air India Flight 182, it has yet to adequately fulfill its obligations under Annex 17.²⁹² Improvements to the regime were prompted mainly by major aviation security incidents which have affected Canada and the US (notably, the bombings of Air India Flight 182 and Pan Am Flight 103 and, especially, the attacks of September 11, 2001). These incidents exposed known weaknesses in the system. There has been little improvement in the security system to anticipate future threats, and the system has failed – in some instances, for decades – to deal with several known security threats.²⁹³

Transport Canada has launched an initiative to review the national civil aviation security regulatory regime in its entirety.²⁹⁴ This is a welcome and important development. Any useful redesign of the system must embrace Annex 17 at its core, in the spirit in which its provisions are intended, and must be informed by international best practices, while addressing any unique threats that Canada faces. Canada must strive to implement timely solutions for significant vulnerabilities and must not wait until solutions are imposed by other regimes or, worse, by an act of terrorism.

3.2.1 International Governance

The international civil aviation security regime has developed primarily in an ad hoc manner, in direct response to particular security incidents. The focus has been on reacting to incidents, not on preventing them.

3.2.1.1 International Regulatory Regime

Modern civil aviation began as the Second World War was nearing an end. The Conference on International Civil Aviation, held in Chicago in 1944, created two organizations that would guide the development of civil aviation in the

²⁹¹ The bombing of Pan Am Flight 103 on December 21, 1988 is a prime example. An employee of Libyan Arab Airlines at Malta's Luqa Airport was implicated in facilitating the acceptance of a bomb-laden unaccompanied suitcase on Air Malta, for interlining to Pan Am in Frankfurt. See Wallis, *Combating Air Terrorism*, p. 38. See also Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4209-4210 and Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4516.

²⁹² Canada does not currently have a written civil aviation security program, nor does it require some of its major security partners and stakeholders to develop and maintain security plans, as required by Annex 17. See Exhibit P-181, p. 3-1, ss. 3.1.1, 3.2, 3.3.1; see also Exhibit P-169, p. 97 of 202.

²⁹³ Experts and stakeholders have repeatedly noted deficiencies in the security measures that address air cargo, airport security, Fixed Base Operations (FBOs) and the General Aviation (GA) sector. See Sections 3.8.1, 3.8.2 and 3.8.3.

²⁹⁴ Exhibit P-101 CAF0827, p. 16 of 19.

coming decades: the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA).²⁹⁵

ICAO is the supreme law-making body for international civil aviation²⁹⁶ and IATA is the not-for-profit trade association for the world's scheduled airlines.²⁹⁷ The establishment of both organizations at the same time was deliberate. It reflected an understanding, from the beginning, of the interdependence of industry and government in civil aviation.²⁹⁸ ICAO was created as the governing body to develop international civil aviation after the war, and it was recognized that a sister organization was required to address commercial aspects of civil aviation.

Security measures cannot be developed in a void and cannot operate in a manner that debilitates the aviation industry. Since their inception, ICAO and IATA have collaborated to advance civil aviation, a shared effort that is viewed as essential. As Rodney Wallis, the former Director of Security at IATA, stated, "...They have to work together because you can't separate the governmental side of civil aviation from the commercial side."²⁹⁹

IATA is formally charged with working alongside ICAO. Besides promoting "...safe, reliable and secure air services for the benefit of the peoples of the world,"³⁰⁰ one of IATA's principal goals, set out in its Articles of Association, is to co-operate with ICAO and other relevant international organizations.³⁰¹ ICAO also acknowledges

²⁹⁵ Wallis, *Combating Air Terrorism*, p. 91. IATA, which had previously been constituted in 1919 as the International Air Traffic Association, was reconceived at the 1944 conference.

²⁹⁶ Wallis, *Combating Air Terrorism*, p. 91.

²⁹⁷ IATA currently represents approximately 250 members: Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8209; see also Wallis, *Combating Air Terrorism*, p. 89.

²⁹⁸ The preamble to the *Convention on International Civil Aviation*, which established ICAO, states, in part that "...the undersigned governments having agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically; Have accordingly concluded this Convention to that end." Exhibit P-150, Preamble, p. 12. One of the stated aims and objectives of ICAO is to "Meet the needs of the peoples of the world for safe, regular, **efficient and economical air transport**" [Emphasis added]: Exhibit P-150, p. 50, Art. 44 d).

²⁹⁹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4214.

³⁰⁰ IATA Articles of Association, adopted as of May 2005, online: IATA <http://www.iata.org/NR/rdonlyres/1C373605-4F10-48C0-81DB-98676881A06A/0/agm61articlesofassociationamended_agm61_tokyo_2931may2005.pdf> (accessed January 14, 2009) [IATA May 2005 Articles of Association]

³⁰¹ The principal goals given to IATA in its original Articles of Association were:
To promote safe, regular and economical air transport for the benefit of the peoples of the world, to foster air commerce and to study the problems connected therewith.
To provide means for collaboration among the air transport enterprises engaged directly or indirectly in international air transport service.
To cooperate with the International Civil Aviation Organization and other international organizations.
As Rodney Wallis noted, although these objectives were set in 1946, long before terrorism became a concern of international civil aviation, they continue to have direct application: Wallis, *Combating Air Terrorism*, pp. 102-103. In IATA's current Articles of Association, the wording of its mission statement has been altered slightly, most notably with respect to the first objective, which now includes reference to security. It states that IATA shall "...[p]romote safe, reliable and secure air services for the benefit of the peoples of the world" [Emphasis added]: IATA May 2005 Articles of Association.

the important contribution to its civil aviation mandate made by IATA and by other international organizations.³⁰² IATA is one of only two non-state members that participate on ICAO's Aviation Security Panel (AVSEC Panel). The Panel reviews ICAO security requirements and recommends changes as necessary.³⁰³ Within its membership, IATA supports and promotes the consistent application of the international security standards and recommended practices established by ICAO. International harmonization of security practices is of particular importance to IATA. Adherence to a common set of international standards ultimately benefits passengers. It provides assurance that security procedures are understood by the international carriers implementing them and that the level of security is consistent across jurisdictions. With a harmonized approach, airlines can focus on ensuring "...the highest level of security standards" rather than on determining which measures to apply in a particular jurisdiction.³⁰⁴

Canada plays a unique role in supporting the ongoing co-operation between ICAO and IATA, since both organizations are headquartered in Montreal.³⁰⁵ In 1945, acting on behalf of the world's governments, Canada's Parliament provided IATA with its current charter.³⁰⁶

Several other international and regional bodies besides ICAO and IATA have a significant impact on civil aviation security. These include the European Civil Aviation Conference (ECAC), whose Security Forum seeks to harmonize civil aviation security policies and practices among its member states.³⁰⁷ Although ECAC is subordinate to ICAO, the political weight of its member states lend it an "...influence far exceeding its numeric strength at the parent body."³⁰⁸ The Airports Council International (ACI) promotes policies and services that strengthen the ability of airports to serve their passengers, customers and communities,³⁰⁹ and is an important and authoritative voice in the civil aviation security community.³¹⁰

³⁰² ICAO reports that it "...works in close collaboration with other specialized agencies of the United Nations such as the International Maritime Organization, the International Telecommunication Union and the World Meteorological Organization. The International Air Transport Association, the Airports Council International, the International Federation of Air Line Pilots' Associations and other international organizations participate in many ICAO meetings." See ICAO Backgrounder, p. 5.

³⁰³ In the wake of the liquid and gel explosives threat that was uncovered in the United Kingdom in August 2006, ICAO convened an extraordinary meeting of its Council, and IATA worked closely with ICAO's AVSEC Panel to develop harmonized regulations that could be applied in all jurisdictions of the world, to simplify the procedures that both airlines and passengers would have to follow: Testimony of Georgina Graham, vol. 66, October 25, 2007, pp. 8210-8211.

³⁰⁴ Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8211.

³⁰⁵ Wallis, *Combating Air Terrorism*, p. 89.

³⁰⁶ Wallis, *Combating Air Terrorism*, p. 102.

³⁰⁷ Exhibit P-101 CAF0831, p. 7 of 8.

³⁰⁸ Wallis, *Combating Air Terrorism*, p. 89.

³⁰⁹ Exhibit P-101 CAF0831, p. 8 of 8.

³¹⁰ Wallis, *Combating Air Terrorism*, p. 90.

3.2.1.1.1 International Conventions

ICAO was established by the *Chicago Convention*, which serves as the foundation for all international civil aviation operations.³¹¹ It specifies the privileges and restrictions that pertain to all signatories, or Contracting States, and provides for the adoption of international standards and recommended practices in all areas of civil aviation.

ICAO is an agency of the United Nations. Its membership consists of sovereign nations. Currently, 190 Contracting States³¹² together comprise ICAO's main body, the Assembly, which meets once every three years.³¹³ The Assembly adopts resolutions, but does not set the international rules with which members must comply. The Council, ICAO's governing body, converts Assembly resolutions into international standards and recommended practices. The Council consists of 36 nations elected from the Assembly for a three-year term, with representation to ensure that those states with the greatest involvement in civil aviation enjoy majority participation and that the main geographic areas of the world are represented.³¹⁴

The international standards and recommended practices adopted by the ICAO Council are published in Annexes to the *Chicago Convention*. Since 1944, 18 Annexes have been added to the Convention, each pertaining to a different area of civil aviation, such as aircraft operation, licensing, air worthiness and meteorology.³¹⁵ Standards are mandatory provisions with which all signatories to the Convention must comply.³¹⁶ Recommended practices are not obligatory, but are considered desirable measures³¹⁷ that should be adopted by states that have the ability to do so.³¹⁸

³¹¹ Wallis, *Combating Air Terrorism*, p. 91.

³¹² Online: International Civil Aviation Organization < http://www.icao.int/cgi/goto_m.pl?cgi/statesDB4.pl?en > (accessed January 14, 2009).

³¹³ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4216.

³¹⁴ Two-thirds of the Council is comprised of states that engage the most in civil aviation, while the remaining one-third aims to ensure geographical representation. During their terms of office, Council representatives function as ambassadors to ICAO, operating out of its headquarters. The third main body of ICAO is the Secretariat, which consists of the employees of ICAO, led by the Secretary General: Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4216.

³¹⁵ Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4216-4217; see also ICAO Background, p. 8.

³¹⁶ A Standard is defined in the Eighth Edition of Annex 17 to the *Chicago Convention* (April 2006) as "...[a]ny specification...the uniform application of which is **recognized as necessary** for the safety or regularity of international air navigation and **to which Contracting States will conform** in accordance with the Convention: in the event of impossibility of compliance, notification to the Council is compulsory under Article 38 of the Convention" [Emphasis added]: Exhibit P-181, p. (vi).

³¹⁷ A Recommended Practice is defined in the Eighth Edition of Annex 17 to the *Chicago Convention* (April 2006) as "...[a]ny specification...the uniform application of which is **recognized as desirable** in the interests of safety, regularity or efficiency of international air navigation, and to **which Contracting States will endeavour to conform** in accordance with the Convention" [Emphasis added]: Exhibit P-181, p. (vi).

³¹⁸ Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4216-4217.

The issue of security, addressed in Annex 17, came late to ICAO.³¹⁹ When ICAO was created, air terrorism was not a concern.³²⁰ Flight safety and the economic conditions of civil aviation were the main focus of the developing international regulatory regime.³²¹ Thirty years would pass before security was viewed as being of sufficient interest to the international community to merit a distinct Annex to the Convention. By the late 1960s, the hijacking of aircraft for political ends was occurring with increasing frequency,³²² and three successive and important conventions (in addition to the existing *Chicago Convention*) were drafted in response to specific security incidents. The three conventions provided a network of international rules that covered jurisdiction and the responsibilities of states with respect to “acts of unlawful interference.” As well, ICAO issued a detailed, non-binding security manual to guide states on implementing security measures. Despite these developments, it became clear that the existing regime could not deal adequately with the security threats being encountered,³²³ and Annex 17, *Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, was adopted in 1974.³²⁴ Annex 17 set out the minimum standards for an effective aviation security regime.

The *Convention on Offences and Certain Other Acts Committed on Board Aircraft*,³²⁵ commonly known as the *Tokyo Convention*, was the first to address security in civil aviation. It was not primarily concerned with hijackings or sabotage, preceding the occurrence of many such incidents by several years.³²⁶ Only one provision of the Convention referred to the unlawful seizure of aircraft,³²⁷ demonstrating the low level of concern at the time.³²⁸ The Convention dealt mainly with criminal offences committed on board aircraft. It was enacted in response to a 1960 incident in which a passenger killed another passenger on board an aircraft while it flew over the Atlantic Ocean, but for which there was no legal remedy at the time. The alleged offender could not be prosecuted because international law did not give any state jurisdiction in such circumstances. The *Tokyo Convention* established rules governing jurisdiction over acts or offences committed on board an aircraft while in flight or outside the territory of a state.³²⁹ Under the Convention, jurisdiction is normally given to the state

319 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4215.

320 See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

321 Exhibit P-157, p. 15 of 135.

322 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4211.

323 Exhibit P-157, p. 15 of 135.

324 Exhibit P-151.

325 See Exhibit P-154.

326 Wallis, *Combating Air Terrorism*, p. 92.

327 Exhibit P-154, p. 5, Art. 11(1).

328 Wallis, *Combating Air Terrorism*, p. 92.

329 Exhibit P-154, pp. 3-4, Arts. 1(1)-(2), 3, 4.

of registration of the aircraft.³³⁰ Other states can be granted jurisdiction under certain circumstances.³³¹

The *Tokyo Convention* laid the foundation for government intervention when offences occur on board an aircraft.³³² Although only one provision dealt with the unlawful interference with aircraft, it was nevertheless regarded as an important provision and continues to have relevance.³³³ It required Contracting States to "...take all appropriate measures to restore control of the aircraft to its lawful commander or to preserve his control of the aircraft" in the event of an unlawful seizure.³³⁴ While the inclusion of this provision might have been viewed as a proactive security measure, the potential benefit was negated by the fact that states were slow to ratify the Convention. Signed in 1963, it was unenforceable when a hijacking occurred in 1968 and return of the seized aircraft to its rightful state was not honoured. The Convention needed ratification by one more country before it could come into force. In response, the United States immediately ratified the Convention, and it came into force in 1969.³³⁵

The late 1960s witnessed a rash of aircraft hijackings, and 1970 saw the first coordinated multi-aircraft terrorist hijacking. Three aircraft were destroyed at Dawson's Field in Jordan, as well as one aircraft at Cairo, and hundreds of passengers were taken hostage. This organized attack by the Popular Front for the Liberation of Palestine (PFLP) is generally accepted as the birth of modern-day air terrorism.³³⁶ It was evident that the *Tokyo Convention* could not sufficiently deal with such incidents:

There was a need to specify in an international treaty the action that had to be taken by states when an aircraft was seized unlawfully. The Hague [Convention] did that. Its language recognized the deterrent effect punishment could have on offenders and called on all ICAO contracting states to make the offense "punishable by severe penalties."³³⁷

³³⁰ Exhibit P-154, p. 3, Art. 3.

³³¹ "A Contracting State which is not the State of registration may not interfere with an aircraft in flight in order to exercise its criminal jurisdiction over an offence committed on board except in the following cases: (a) the offence has effect on the territory of such State; (b) the offence has been committed by or against a national or permanent resident of such State; (c) the offence is against the security of such State; (d) the offence consists of a breach of any rules or regulations relating to the flight or maneuver of aircraft in force in such State; (e) the exercise of jurisdiction is necessary to ensure the observance of any obligation of such State under a multilateral international agreement": Exhibit P-154, pp. 3-4, Art. 4.

³³² Wallis, *Combating Air Terrorism*, p. 92.

³³³ Wallis, *Combating Air Terrorism*, p. 92.

³³⁴ Exhibit P-154, p. 5, Art. 11(1).

³³⁵ The United States became the 12th country to ratify the *Tokyo Convention*. Although the *Tokyo Convention* applied to the 1968 hijacking, which occurred in the Middle East, it could not be enforced because only 11 countries had ratified the treaty at that time: Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4225-4226.

³³⁶ Wallis, *Combating Air Terrorism*, p. 92. See also Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

³³⁷ Wallis, *Combating Air Terrorism*, p. 92.

The *Convention for the Suppression of Unlawful Seizure of Aircraft* ("*Hague Convention*") was signed in 1970 and entered into force in 1971.³³⁸ With the alarming growth in aircraft hijackings, the Convention obliged Contracting States to declare hijacking a criminal offence. The goal was to eliminate safe havens for hijackers by imposing a choice on Contracting States for dealing with offenders: prosecute or extradite.³³⁹ In his 1993 book, *Combating Air Terrorism*, Wallis remarked that such strong language made for a powerful treaty, if fully enacted by Contracting States:

If there were no havens to which hijackers could escape after committing their acts of terror, much of their motivation would disappear.

While the *Hague Convention* is viewed as an important development in international civil aviation security, its deterrent effect is no doubt weakened because some governments have failed to live up to their obligations³⁴⁰ and because a new era of suicide terrorism has emerged.

Another limitation of the *Hague Convention* is that it deals only with the hijacking of aircraft. In 1970, as the text for the Convention was being finalized, its drafters recognized that acts of sabotage were not included. Although not as common as hijacking at the time, sabotage was a known method of unlawful interference with civil aviation. Instead of delaying passage of the *Hijacking Convention*, as the *Hague Convention* was also known, ICAO decided to develop a separate treaty to address bombings and similar attacks on aircraft.³⁴¹ A year later, in 1971, the result of its deliberations was the *Suppression of Unlawful Acts against the Safety of Civil Aviation* ("*Montreal Convention*"), which came into effect in 1973.³⁴² The *Montreal Convention* addressed the sabotage of aircraft, whether in flight or on the ground, as well as similar attacks on air navigation facilities.³⁴³ It listed a range of offences to be punished by Contracting States.³⁴⁴ They were also called upon to "...take all practicable measure[s] for the purpose of preventing the offences" specified in the Convention.³⁴⁵ This proved to be a valuable clause, since it gave the airline industry the authority for its efforts to enhance airport security around the world. It also gave ICAO a springboard for launching Annex 17 to the *Chicago Convention*.³⁴⁶

The *Montreal Convention* did not cover all sabotage against civil aviation. This became apparent after simultaneous attacks at the airport terminals in Rome

³³⁸ See Exhibit P-155, pp. 1-2.

³³⁹ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4226.

³⁴⁰ Wallis, *Combating Air Terrorism*, p. 93.

³⁴¹ Wallis, *Combating Air Terrorism*, p. 94.

³⁴² See Exhibit P-156, pp. 1-2.

³⁴³ Exhibit P-156, p. 2, Art. 1.

³⁴⁴ Exhibit P-156, pp. 5-6, Arts. 3, 8; see also Wallis, *Combating Air Terrorism*, pp. 94-95.

³⁴⁵ Exhibit P-156, p. 7, Art. 10.

³⁴⁶ Wallis, *Combating Air Terrorism*, p. 95.

and Vienna in December 1985.³⁴⁷ The Council of ICAO wanted to invoke the *Montreal Convention*, but realized this was not possible since the treaty did not address public areas of airports. Only the local police had jurisdiction over these incidents.³⁴⁸ This void in authority over a matter concerning aviation terrorism prompted the development, in 1988, of the *Montreal Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*. The Montreal Protocol, as it is commonly known, adds to and amends the *Montreal Convention* to create uniform legislation for the suppression of terrorist attacks at airports. It should be read with the Montreal Convention as a single instrument.³⁴⁹

The most recent ICAO convention in aviation security stemmed, once again, from a major incident. The destruction of Pan Am Flight 103 on December 21, 1988, was caused by plastic explosives concealed in unaccompanied, interlined baggage. Although it was well known that plastic explosives were difficult to detect using existing X-ray equipment, and intelligence reports at the time had warned specifically about the imminent use of plastic explosives to target an aircraft in flight,³⁵⁰ local Pan Am management staff chose X-ray scanning as the sole method to screen interlined baggage for explosives.³⁵¹ The baggage containing the explosives slipped undetected onto Flight 103. Following the bombing, ICAO developed the *Convention on the Marking of Plastic Explosives for the Purpose of Detection*. The Convention prohibits the manufacture, sale or possession of plastic explosives without the chemical markings specified by the Convention. These markings make it easier for screening equipment to detect the explosives. Signed in 1991, the Convention came into force in 1998.³⁵²

As well as developing conventions to address civil aviation security, the Council of ICAO decided in 1969 to establish the Committee on Unlawful Interference, observing that the threat posed to civil aviation required the urgent and continued attention of ICAO.³⁵³ The Committee is comprised of a subset of Council members³⁵⁴ who review incidents of hijacking and sabotage and submit recommendations to the Council.³⁵⁵

3.2.1.1.2 Annex 17 and the ICAO Security Manual

In 1968, in response to a number of hijackings related to Cuba, ICAO convened an *ad hoc* group of experts to prepare a security manual that could assist Contracting States in addressing acts of unlawful interference with international

³⁴⁷ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

³⁴⁸ Testimony of Moses Aléman, May 29, 2007, p. 4227.

³⁴⁹ Exhibit P-263, Tab 3, p. 2 of 3.

³⁵⁰ Wallis, *Lockerbie*, p. 23.

³⁵¹ Wallis, *Lockerbie*, p. 104.

³⁵² Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4228.

³⁵³ ICAO 1969 News Release, online: International Civil Aviation Organization <http://www.icao.int/icao/en/nr/1969/pio196904_e.pdf>, p. 2 (accessed January 14, 2009) [ICAO 1969 News Release].

³⁵⁴ ICAO 1969 News Release, p. 2.

³⁵⁵ ICAO 1969 News Release, p. 4.

civil aviation. First published in 1971,³⁵⁶ the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference* (Security Manual) was purely a guide for states and security stakeholders. The measures it outlined were not binding, since the Security Manual did not have any official regulatory status.³⁵⁷

After Annex 17 came into existence in 1974, the Security Manual could be used to assist states in applying the Annex and to provide governments, airports and air carriers with practical guidance for meeting their security responsibilities.³⁵⁸ Annex 17 and the Security Manual are meant to be companion documents.³⁵⁹ Annex 17 uses broad language to describe the desired outcomes of its standards and recommended practices, while the Security Manual provides specific ways for states and their security partners to accomplish these objectives.

Unlike Annex 17, the Security Manual is a lengthy document that specifies in detail several methods for implementing various security measures, from the simplest and most cost-efficient options for states with fewer resources, to the more sophisticated procedures that wealthier states may be able to afford.³⁶⁰ The Security Manual includes guidance about the security measures required of most partners in civil aviation security, such as airports, air carriers, security officers and police. The Manual is a restricted document provided by ICAO to Transport Canada, and only Transport Canada has the authority to share its contents.³⁶¹

³⁵⁶ Subsequent amendments were made in 1974, 1977 and 1983. See Exhibit P-157, p. 17 of 135.

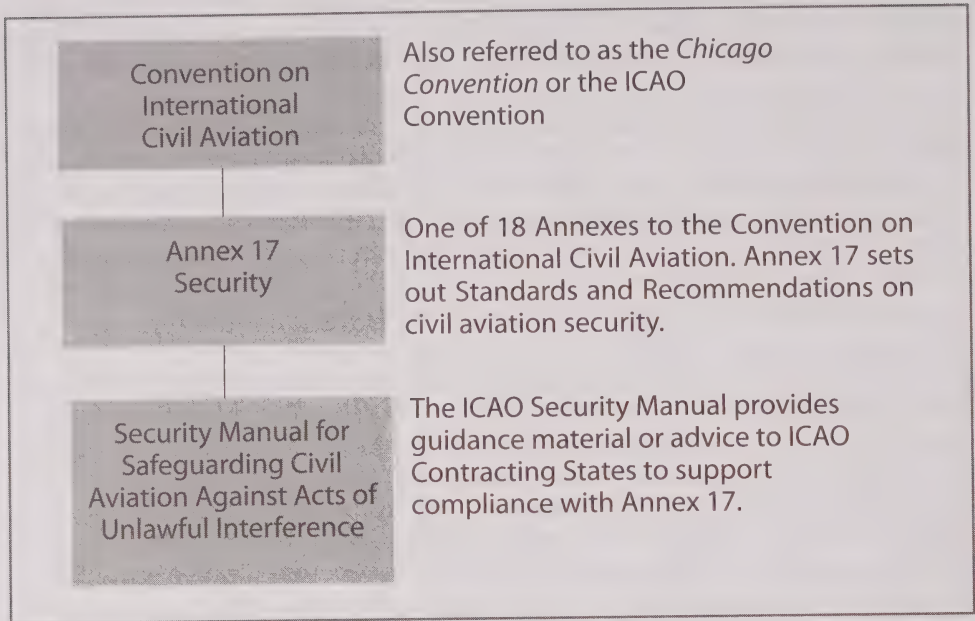
³⁵⁷ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4211.

³⁵⁸ Exhibit P-157, p. 17 of 135.

³⁵⁹ Indeed, the Security Manual is specifically referenced throughout the text of Annex 17 as a guidance document to assist with the implementation of various standards. See Exhibit P-181, pp. (v) and 2-1–4-3. See also Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4278.

³⁶⁰ Testimony of Moses Aléman, vol. 36, May 30, 2007, pp. 4278-4279.

³⁶¹ The Security Manual is provided only to a state's designated authority as specified under Standard 3.1.2 of Annex 17. See Exhibit P-181, p. 3-1, s. 3.1.2. See also Testimony of Moses Aléman, vol. 36, May 30, 2007, pp. 4278-4279.

Figure 1: International Aviation Security Regulatory Framework

The first edition of Annex 17, adopted in 1974, established the international standards and recommended practices that were to comprise the minimum security framework expected of all Contracting States.³⁶² The first edition, however, consisted primarily of recommendations, which are akin to best practices³⁶³ and are optional.³⁶⁴ Some experts who appeared before the Commission viewed this edition of the Annex as a substandard document that did not give states the means to meet the myriad security threats facing civil aviation.³⁶⁵ Very little was added to Annex 17 in its second edition, which was adopted in 1981³⁶⁶ and which was the edition in force when Air India Flight 182 was destroyed.³⁶⁷ Only then did ICAO recognize that Annex 17 did not adequately address the threats to civil aviation and that a much more robust document was necessary.³⁶⁸ A wholesale revision of Annex 17 ensued.³⁶⁹

³⁶² Exhibit P-157, p. 16 of 135. Although adopted in 1974, Annex 17 did not come into effect until 1975. See Exhibit P-151. See also Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

³⁶³ Exhibit P-157, p. 16 of 135.

³⁶⁴ Wallis, *Combating Air Terrorism*, p. 97.

³⁶⁵ See, for example, Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

³⁶⁶ See Exhibit P-152.

³⁶⁷ In 1985, Annex 17 obliged Contracting States to "...take the necessary measures to prevent weapons or any other dangerous devices, the carriage or bearing of which is not authorized, from being introduced, by any means whatsoever, on board an aircraft engaged in the carriage of passengers": Exhibit P-152, Standard 4.1.5. It recommended "...the necessary procedures to prevent the unauthorized introduction of explosives or incendiary devices in baggage, cargo, mail and stores to be carried on board aircraft" and further recommended measures to protect the same between the terminal buildings and aircraft "...with the view to safeguarding such aircraft against acts of sabotage": Exhibit P-152, Recommendation 4.1.14 and Recommendation 4.1.16.

³⁶⁸ Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4217-4218.

³⁶⁹ See, for example, Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

ICAO named an *ad hoc* group of international security experts, initially from 16 nations and four international organizations, to revise Annex 17. The revised Annex adopted 35 standards, where previously there were only 13.³⁷⁰ The group was also required to meet periodically to review Annex 17 and to consider whether new standards should be adopted and whether recommended practices needed to be elevated to the status of standards.³⁷¹ The group eventually became known as the AVSEC Panel,³⁷² which served as a specialist security body, with membership drawn from states and international organizations, and reported to the Committee on Unlawful Interference.³⁷³

Annex 17 has been described as "...a small, singularly simple publication but one born out of much debate in order to balance the perceived needs of civil aviation seen through the eyes of security specialists (the AVSEC Panel), against the political and economic considerations of the members of the ICAO Committee on Unlawful Interference and the Council."³⁷⁴ The current edition of Annex 17 was adopted in 2005 and came into effect in April 2006.³⁷⁵ It is organized into five main chapters that address the following: (1) definitions, to clarify key terminology used in international civil aviation security; (2) general principles; (3) the organization of national regimes; (4) preventive security measures; and (5) the management of responses to acts of unlawful interference.³⁷⁶ Most nations, including Canada, are signatories to the Chicago Convention,³⁷⁷ and Annex 17 is the core document from which all national civil aviation security regimes must flow. It provides a blueprint for the essential elements that comprise a basic, but inclusive, regime. Among other obligations under Annex 17, Contracting States are required to:

- Establish an organization and develop and implement regulations, practices and procedures for safeguarding civil aviation against acts of unlawful interference;³⁷⁸
- Establish and implement a written national civil aviation security program;³⁷⁹
- Designate and specify to ICAO an appropriate authority with responsibility for developing, implementing and maintaining the national civil aviation security program;³⁸⁰
- Establish a national aviation security committee to coordinate security activities between all entities with responsibilities within the national civil aviation security program;³⁸¹

370 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

371 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

372 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

373 Wallis, *Combating Air Terrorism*, p. 90.

374 Wallis, *Combating Air Terrorism*, p. 97.

375 Exhibit P-181, p. (viii).

376 Exhibit P-181, p. (iii).

377 See Exhibit P-452.

378 Exhibit P-181, p. 2-1, s. 2.1.2.

379 Exhibit P-181, p. 3-1, s. 3.1.1.

380 Exhibit P-181, p. 3-1, s. 3.1.2.

381 Exhibit P-181, p. 3-1, s. 3.1.5.

- Require all airports³⁸² and commercial air carriers³⁸³ to establish, implement and maintain a written security program for their operations that meets the requirements of the national civil aviation security program;
- Ensure that each airport establishes an airport security committee to assist in implementing the airport security program;³⁸⁴
- Establish measures to prevent unauthorized weapons, explosives or anything that could unlawfully interfere with civil aviation from being introduced on board an aircraft,³⁸⁵ including measures relating to:
 - Access control, particularly non-passenger and vehicular access to airside and restricted areas of airports, through means such as identification systems, background checks, appropriate supervision and the screening of at least a proportion of non-passengers and their belongings;³⁸⁶
 - Aircraft security, including conducting aircraft security checks and protecting the flight crew compartment;³⁸⁷
 - Screening and protection of passengers and their cabin baggage;³⁸⁸
 - Screening and protection of hold baggage, including ensuring that the baggage of any passenger not on board an aircraft is not transported unless appropriately identified and screened;³⁸⁹
 - Screening and protection of cargo and mail³⁹⁰ and the application of security controls to catering, stores and supplies³⁹¹ carried on passenger aircraft;
- Ensure, to the extent practicable, that security measures are applied based upon a security risk assessment carried out by the relevant national authorities;³⁹²
- Ensure the development and implementation of a national training program for the personnel of all entities with responsibility for aspects of the national civil aviation security program;³⁹³

³⁸² Exhibit P-181, p. 3-1, s. 3.2.1.

³⁸³ Exhibit P-181, p. 3-1, s. 3.3.1.

³⁸⁴ Exhibit P-181, p. 3-1, s. 3.2.3.

³⁸⁵ Exhibit P-181, p. 4-1, s. 4.1.

³⁸⁶ See Exhibit P-181, p. 4-1, ss. 4.2.1-4.2.6.

³⁸⁷ See Exhibit P-181, p. 4-1, ss. 4.3.1-4.3.3.

³⁸⁸ See Exhibit P-181, pp. 4-1-4-2, s. 4.4.1-4.4.4.

³⁸⁹ See Exhibit P-181, p. 4-2, s. 4.5.1-4.5.5.

³⁹⁰ This includes a process for approving regulated agents if such a program is established by a Contracting State. See Exhibit P-181, p. 4-2, ss. 4.6.1-4.6.4.

³⁹¹ See Exhibit P-181, p. 4-2, s. 4.6.5.

³⁹² Exhibit P-181, p. 2-1, s. 2.2.2.

³⁹³ Exhibit P-181, p. 3-1, s. 3.1.6.

- Develop and maintain a national civil aviation security quality control program to assess compliance with and to validate the effectiveness of its national civil aviation security program;³⁹⁴
- Constantly review the level of threat to civil aviation within its territory and adjust relevant elements of its national civil aviation security program accordingly;³⁹⁵ and
- Co-operate with other states in developing and exchanging information concerning national civil aviation security, training and quality control programs, as necessary.³⁹⁶

3.2.1.2 *Limitations on International Governance*

Several concerns have been raised about ICAO governance in civil aviation security, such as its political constitution, which can hinder decision-making and result in the appointment of representatives poorly qualified to work in this highly technical and specialized field. As with other international bodies with representatives from nations, ICAO is seen as a political organization. The language developed to govern international civil aviation is necessarily based on compromise.³⁹⁷ Any rules adopted require consensus³⁹⁸ and must enable those states with the fewest resources to comply.³⁹⁹ Wallis has described the problem of resources:

Sometimes the words are weak because the country simply doesn't have money to do things. You might have a country that has to make a decision between having an X-ray machine at an airport and an X-ray machine in a hospital. They might opt to have an X-ray machine in the hospital but in a developed country you would expect them to have all of these things, and they could push ahead.⁴⁰⁰

The process of establishing standards can prove frustrating. Annex 17 security provisions often fail to find acceptance on anything more than the level of the "lowest common denominator."⁴⁰¹ Inevitably, the wording chosen for international standards gives states considerable freedom in implementing them.⁴⁰²

ICAO standards must be considered minimum standards that states with the requisite resources, particularly developed countries, should be able to easily

394 Exhibit P-181, p. 3-1, s. 3.4.4.

395 Exhibit P-181, p. 3-1, s. 3.1.3.

396 Exhibit P-181, p. 2-1, s. 2.4.2.

397 Wallis, *Combating Air Terrorism*, p. 91.

398 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4218.

399 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4218.

400 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4218.

401 Wallis, *Combating Air Terrorism*, p. 91; Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4285.

402 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4218.

exceed.⁴⁰³ Exceeding these standards, where it is possible to do so, appears to have been a long-established practice. Before the bombing of Air India Flight 182, Canada, the US and many European nations had established national regimes exceeding the standards in Annex 17.⁴⁰⁴ Aviation security reviews and investigations concluded that Canada had exceeded Annex 17 standards at the time of the Air bombings. This should have been no surprise, although Transport Canada officials often mentioned it as being particularly noteworthy.⁴⁰⁵

There is also concern that government representatives who serve ICAO's main bodies and committees are drawn from the civil service and often lack substantial background in civil aviation security.⁴⁰⁶ The Committee on Unlawful Interference consists of ICAO Council members who function much like national ambassadors and whose security backgrounds may be minimal or non-existent.⁴⁰⁷ Yet this Committee finalizes recommendations to be put to the Council to provide direction in aviation security.⁴⁰⁸ In contrast, IATA established a Security Advisory Committee (SAC) in 1967, with goals similar to ICAO's Committee on Unlawful Interference, but with a notably different composition. Formed to develop collective airline policies to combat air terrorism, the SAC, later renamed the Security Advisory Group, consisted of experts in civil aviation security. These were drawn from among the security heads of international airlines.⁴⁰⁹

Despite its limitations, ICAO has produced important international legal instruments to manage civil aviation security, although these have largely developed in an *ad hoc* and reactive fashion. Since 1985, the Committee on Unlawful Interference has sought guidance from the AVSEC Panel, which consists of security experts from several states and organizations,⁴¹⁰ including IATA.⁴¹¹ The AVSEC Panel authored the first substantial rewrite of Annex 17 after the destruction of Air India Flight 182,⁴¹² introducing a much more rigorous regime of international civil aviation security standards.⁴¹³ Experts in security were added to advise the Committee on Unlawful Interference. This was a welcome development, and its continued influence in matters of security, particularly related to Annex 17,⁴¹⁴ might help to balance the deficiencies associated with other ICAO bodies that have responsibilities in civil aviation security. However, even though the AVSEC Panel provides specialist knowledge, only the individual Contracting States, through their representatives, have the authority to finalize ICAO rules.⁴¹⁵ Their decisions can be swayed by competing interests and may

403 Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4271.

404 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

405 Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4501.

406 Wallis, *Combating Air Terrorism*, p. 104.

407 Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4216-4217.

408 Wallis, *Combating Air Terrorism*, pp. 90, 104.

409 See Wallis, *Combating Air Terrorism*, pp. 103-104.

410 Wallis, *Combating Air Terrorism*, p. 90.

411 Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8210.

412 Wallis, *Combating Air Terrorism*, p. 90.

413 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4241.

414 Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4217.

415 Wallis, *Combating Air Terrorism*, p. 90.

not be informed by the appropriate expertise. This is an inherent limitation of the process for developing standards.

A further limitation is that the international civil aviation security regime does not provide for any mechanism of enforcement. This is an issue of sovereignty. Despite the obligation on signatories of the *Chicago Convention* to comply with Annex 17, there is no mechanism to force states to comply:

There is no penalty or sanction provided by ICAO. ICAO has refused throughout the years to become an international policeman. The reasoning that they use is that it is an international organization of sovereign countries and every country is left to apply the standards in their own method....⁴¹⁶

A formal mechanism exists for states to opt out of implementing an Annex 17 standard. Under Article 38 of the *Chicago Convention*, states are obliged to notify the Council of ICAO of any departures from the international standards:

Any State which finds it impracticable to comply in all respects with any such international standard or procedure, or to bring its own regulations or practices into full accord with any international standard or procedure after amendment of the latter, or which deems it necessary to adopt regulations or practices differing in any particular respect from those established by an international standard, shall give immediate notification to the International Civil Aviation Organization of the differences between its own practice and that established by the international standard.... In any such case, the Council shall make immediate notification to all other states of the difference which exists between one or more features of an international standard and the corresponding national practice of that State.⁴¹⁷

States may be unable or unwilling to comply with an Annex 17 standard for several reasons. One may be financial:

The state may simply not have the money to implement the procedures called for by the annex. This is often so in developing countries. A government could quite literally be faced with a choice of providing a new security facility or feeding a hungry or even starving population. It becomes a matter of priorities.⁴¹⁸

⁴¹⁶ Testimony of Moses Aléman, vol. 36, May 30, 2007, pp. 4274-4275.

⁴¹⁷ Exhibit P-150, pp. 44-46, Art. 38.

⁴¹⁸ Wallis, *Combating Air Terrorism*, p. 98.

ICAO standards, as noted, are essentially set at the level of the lowest common denominator to accommodate the states with the least means. This should keep to a minimum the number of states that lack the resources to comply with Annex 17.⁴¹⁹ But other operational, administrative and political considerations also come into play. A delegate to ICAO might “vote with the mood of those present”⁴²⁰ when a rule is adopted, only to discover later that it is not possible to implement the rule domestically. Other times, a state representative may lack the authority or influence to put ICAO decisions into practice. It may also be that the implications of a rule were not fully understood at the time of its adoption. Although ICAO conducts its meetings in several official languages, some delegates may end up using a language with which they are not completely familiar and may not grasp the subtleties of debates as a result. Further reflection and an opportunity for discussion in home surroundings may reveal unforeseen obstacles. It could also be that a state disagrees with the rule from the beginning but chooses not to say so in an open forum.⁴²¹

The formal procedure for notifying ICAO of a failure to meet international standards is termed “filing a difference.”⁴²² The state must notify the Council of ICAO and provide details of the differences between the standard and its national regulations.⁴²³ Typically, ICAO publishes a list of states that have filed differences and specifies the nature of the discrepancies.⁴²⁴ The publication of differences works effectively for annexes that deal with other matters in civil aviation, but security issues are confidential and must be treated in a more circumspect manner to avoid information falling into the wrong hands. Differences filed in civil aviation security are not published, but are shared with the designated authorities of all signatories to the *Chicago Convention*.⁴²⁵ Each state can then determine how this information should be used, to whom it should be disseminated and whether its own security requirements must be altered in response. ICAO does not interfere with such decisions, as these are considered state matters.⁴²⁶ The filing of differences can result in the loss of insurance coverage or the loss of access to services because of blacklisting by other countries.⁴²⁷

ICAO publications, even those marked “restricted,” have wide circulation.⁴²⁸ Moreover, rogue states that are members of ICAO, or rogue airlines that are members of IATA, will be privy to any security-sensitive information discussed or shared within these organizations. There is no fail-safe method of preventing such documents from reaching terrorists. All security programs must be designed so that measures remain effective even if terrorists have knowledge

⁴¹⁹ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4285.

⁴²⁰ Wallis, *Combating Air Terrorism*, p. 97.

⁴²¹ Wallis, *Combating Air Terrorism*, p. 97.

⁴²² Wallis, *Combating Air Terrorism*, p. 97.

⁴²³ Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4273.

⁴²⁴ Wallis, *Combating Air Terrorism*, p. 97.

⁴²⁵ Testimony of Moses Aléman, vol. 36, May 30, 2007, pp. 4282-4283.

⁴²⁶ Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4285.

⁴²⁷ Exhibit P-157, p. 16 of 135.

⁴²⁸ Wallis, *Combating Air Terrorism*, p. 98.

of them.⁴²⁹ However, information relating to the filing of differences presents a particular problem:

...[I]f a state indicated, for example, that it could not comply with the standard calling for reconciliation of passengers with their baggage, terrorists would be able to identify this loop-hole and attack civil aviation operations through it.⁴³⁰

At least ICAO's restriction of civil aviation security information makes it more difficult than it would otherwise be for terrorists to obtain and misuse the information.⁴³¹

The Commission was informed that some states have filed differences with ICAO in relation to Annex 17, but the current status or content of those differences is not known.⁴³² The Commission was further informed that states do not always file differences because they may be reluctant to admit that they are not complying with standards.⁴³³ This can endanger the security of other states and air carriers that may unknowingly be exposed to security weaknesses because of the inaction of the offending state.⁴³⁴

In practice, international airlines are often aware of security deficiencies, even if ICAO is not informed, simply because they conduct security operations around the world.⁴³⁵ Their employees work and reside in various jurisdictions and can observe whether standards are met.⁴³⁶ Airport security committees become an important place for airlines and other stakeholders to openly discuss their concerns about security.⁴³⁷

Oversight in international civil aviation security matters is limited. Annex 17 sets only minimum standards, and there is no mechanism to compel compliance. Reliance on airport security committees is not sufficient to make up for deficiencies in oversight.⁴³⁸

Although ICAO has no means to enforce its rules, improved oversight became available through the Universal Security Audit Program (USAP) developed after September 11, 2001. The USAP's initial objective was to assess compliance with Annex 17 standards by reviewing the aviation security regimes of Contracting States, as well as by examining airport security on a sample basis.⁴³⁹ Canada

⁴²⁹ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4277.

⁴³⁰ Wallis, *Combating Air Terrorism*, p. 98.

⁴³¹ Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4279.

⁴³² Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4283.

⁴³³ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4285.

⁴³⁴ Wallis, *Combating Air Terrorism*, p. 98.

⁴³⁵ Testimony of Rodney Wallis, vol. 36, May 30, 2007, pp. 4285-4286.

⁴³⁶ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4286.

⁴³⁷ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4286.

⁴³⁸ Exhibit P-181, p. 3-1, s. 3.2.2.

⁴³⁹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4734.

was audited by ICAO under the USAP in 2005. Canada prepared a Corrective Action Plan in response and, in 2007, ICAO reviewed Canada's progress.⁴⁴⁰ The agreement between ICAO and member states does not permit making USAP findings and recommendations public.⁴⁴¹

In May 2008, Transport Canada officials advised the Commission that ICAO had completed a full cycle of audits. In other words, all Contracting States had been audited under the USAP. Future ICAO audits will no longer review national aviation security regimes, but instead will review the ability of states to audit their own regimes.⁴⁴² ICAO audits will review the practices and procedures that enable states to oversee their national aviation security systems.⁴⁴³

3.2.2 Oversight of Aviation Security in Canada

The Government of Canada named Transport Canada as the designated authority responsible for national civil aviation security,⁴⁴⁴ and its officials represent Canada at ICAO.⁴⁴⁵ Under its civil aviation security mandate, Transport Canada is responsible for:

- Developing aviation security policy, including the designation of airports for CATSA screening;
- Developing the *Canadian Aviation Security Regulations* for Governor-in-Council approval;
- Adopting security Measures, Orders, Emergency Directions and Interim Orders;
- Monitoring the aviation industry to ensure compliance;
- Managing the Airport Restricted Area Access Clearance Program; and
- Working with intelligence agencies⁴⁴⁶ to provide intelligence to CATSA, airport operators and air carriers.⁴⁴⁷

Although Transport Canada, as noted earlier, is the ultimate domestic authority in civil aviation security, operational responsibility for security is shared by several federal government departments and agencies, air carriers, airport operators and many other stakeholders. It is an integrated system that involves government, private sector⁴⁴⁸ and not-for-profit

⁴⁴⁰ Exhibit P-101 CAF0827, p. 11 of 19.

⁴⁴¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4714.

⁴⁴² Exhibit P-101 CAF0827, p. 13 of 19.

⁴⁴³ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4711.

⁴⁴⁴ Exhibit P-181, p.

⁴⁴⁵ Exhibit P-169, p. 30 of 202.

⁴⁴⁶ The main intelligence agencies with which Transport Canada collaborates are CSIS, the RCMP and ITAC.

See Exhibit P-169, p. 30 of 202, note 24.

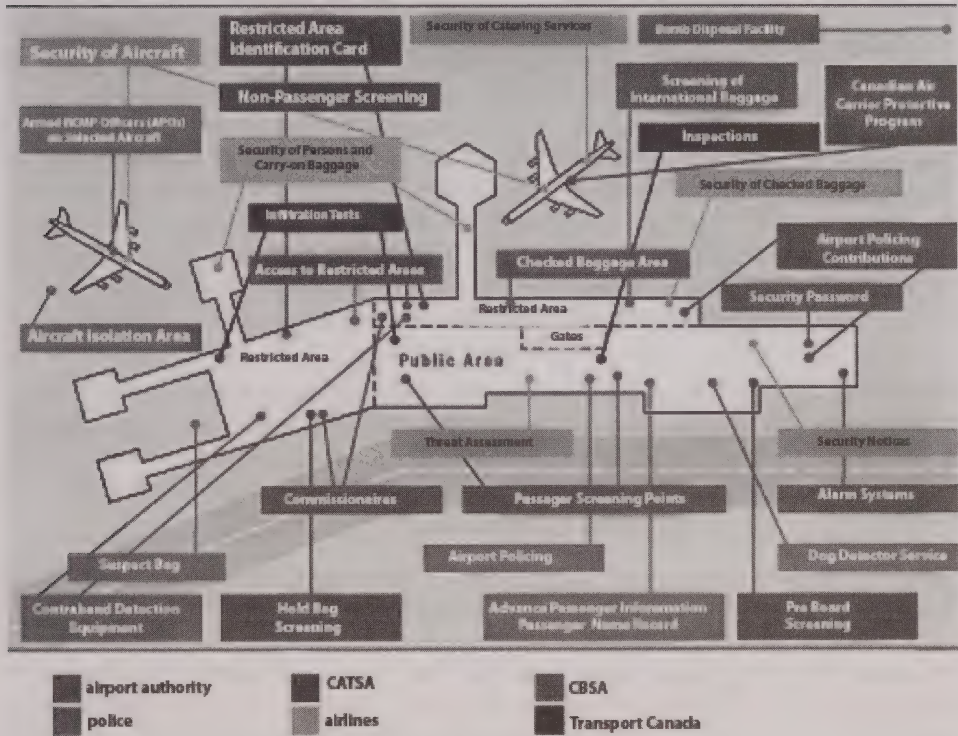
⁴⁴⁷ Exhibit P-169, p. 30 of 202.

⁴⁴⁸ Exhibit P-169, p. 31 of 202.

organizations.⁴⁴⁹ These include retail establishments, FBOs and ground-handling service providers. Figure 2 illustrates the complexity of security operations and the different organizations often involved at the airport level.

Figure 2: The Airport Security Environment

2.1 The airport security environment



Source: Canadian Air Transport Security Authority Act Review Advisory Panel, *Flight Plan: Managing the Risks in Aviation Security - Report of the Advisory Panel* (2006), Exhibit P-169, p. 27.

Note: CBSA is the Canada Border Services Agency.

Transport Canada has a broad mandate, with responsibility for all major modes of transportation, including civil aviation.⁴⁵⁰ Because security is not the Department's sole concern, some observers have questioned its suitability to have primary responsibility in civil aviation security.

In its 2007 report on airport security in Canada, the Standing Senate Committee on National Security and Defence (Senate Committee) was critical of leaving

⁴⁴⁹ Airport authorities are incorporated as not-for-profit organizations: Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8139.

⁴⁵⁰ Exhibit P-169, p. 35 of 202.

aviation security matters with Transport Canada. The Committee spoke of the incompatible interests of security and industry:

Transport Canada should get out of the security field and focus on areas in which it has competence, [like] making Canada's transportation network more efficient. This is what Transport Canada is really interested in – moving people and things with maximum [efficiency]. The Committee is not saying that this is not a worthy pursuit. It surely is.

But others should be in charge of security, primarily because the need for proper security sometimes gets in the way of moving people and things as quickly as they could be moved without proper security. Putting Transport Canada in charge of security is comparable to putting Industry Canada in charge of the environment. Industry Canada wants maximum production. Environmentalists want to ensure that production doesn't despoil the planet. The roles don't mix.⁴⁵¹

The Senate Committee recommended that Transport Canada be relieved of its responsibility for security at airports and that this responsibility be transferred to the Department of Public Safety and Emergency Preparedness Canada (now Public Safety Canada),⁴⁵² which was created after the events of September 11, 2001.⁴⁵³

The Committee's view is not widely shared. The establishment of ICAO and IATA at the same conference in Chicago in 1944 acknowledged the need in civil aviation for ongoing collaboration between those who regulate and those who implement.⁴⁵⁴ While governments set the rules, consideration must be given to their feasibility within the air transport industry. In 1985, the Seaborn Report, which undertook a comprehensive review of aviation security in Canada after the bombing of Air India Flight 182, spoke of the need for "...a reasonable balance between the expeditious movement of passengers and the assurance of their safety and security"⁴⁵⁵ and stressed the importance of "...practical means of improving airport and airline security."⁴⁵⁶ Efficient air travel and effective aviation security, the report said, must be accomplished together:

The threat of terrorism must not be permitted unduly to interfere with the normal activities of daily life, including air travel. It must, however, be recognized that air travellers are vulnerable to terrorist and other similar attacks. It is, therefore,

⁴⁵¹ Exhibit P-172, p. 63 of 155.

⁴⁵² Exhibit P-172, p. 64 of 155.

⁴⁵³ Exhibit P-169, p. 35 of 202.

⁴⁵⁴ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4214.

⁴⁵⁵ Exhibit P-101 CAF0039, p. 2 of 10.

⁴⁵⁶ Exhibit P-101 CAF0039, p. 2 of 10.

most important that air security be based on efficient as well as effective means, as a matter of routine, of security checking large numbers of persons and their baggage as well as air cargo and mail.⁴⁵⁷

This issue recently received comprehensive consideration as part of an independent five-year review of the *Canadian Air Transport Security Authority Act (CATSA Act)*.⁴⁵⁸ Based on the recommendations of the CATSA Act Review Advisory Panel (CATSA Advisory Panel), the Government decided that authority over civil aviation security would remain with Transport Canada.⁴⁵⁹ The CATSA Advisory Panel echoed the sentiments of the Seaborn Report, saying that most stakeholders stressed the importance of an economically viable civil aviation sector that maintained public service while providing the highest standards of security.⁴⁶⁰ The Panel stated that most members of the travelling public also wished to see security as part of an efficient and comfortable system of air travel.⁴⁶¹ Indeed, Annex 17 requires states to implement their security regulations, practices and procedures while taking into account the “regularity” and efficiency of flights.⁴⁶² This is emphasized in Recommended Practice 2.3:

*Each Contracting State should whenever possible arrange for the security controls and procedures to cause a minimum of interference with, or delay to the activities of, civil aviation provided the effectiveness of these controls and procedures is not compromised.*⁴⁶³ [Emphasis in original]

The Panel found little support and “few compelling arguments”⁴⁶⁴ from stakeholders or interested parties for a change in governance for civil aviation security.⁴⁶⁵ It noted that Transport Canada’s situation is analogous to the arrangement in the UK, where the Department of Transport is the designated national authority, but differs from that of the US, where the Transportation Security Administration (TSA) is part of the Department of Homeland Security (DHS), which is separate from the US Department of Transportation.⁴⁶⁶ The Panel reported that the consensus among stakeholders and others with an interest in civil aviation was that Transport Canada, with its mandate for the transportation

⁴⁵⁷ Exhibit P-101 CAF0039.

⁴⁵⁸ See Exhibit P-169.

⁴⁵⁹ Exhibit P-101 CAF0871, p. 1 of 4.

⁴⁶⁰ Exhibit P-169, p. 23 of 202.

⁴⁶¹ Exhibit P-169, p. 23 of 202.

⁴⁶² Exhibit P-181, p. 2-1, s. 2.1.2.

⁴⁶³ Exhibit P-181, Recommended Practice 2.3, p. 2-1. Note: In order to easily differentiate Recommended Practices from Standards in Annex 17, the former are printed in italics and are accompanied by the prefix “**Recommendation**” [Emphasis in original]: Exhibit P-181, p. (vi).

⁴⁶⁴ Exhibit P-169, p. 35 of 202.

⁴⁶⁵ Exhibit P-169, p. 35 of 202.

⁴⁶⁶ The federal responsibility for passenger and baggage screening was transferred from the Federal Aviation Administration (FAA) to the TSA in November 2001, in the wake of the events of September 11, 2001. See Exhibit P-157, p. 96 of 135; Exhibit P-169, p. 34 of 202.

sector as a whole, was the most appropriate authority for aviation security and could best integrate security with more general transportation policy.⁴⁶⁷

The Commission agrees that civil aviation security measures must enable the air travel industry to continue to operate efficiently, and that Transport Canada is best placed to pursue both security and efficiency, even if these objectives sometimes compete. It must do so, however, with ever-vigilant regulatory oversight that will foster a common vision for aviation security and true collaboration among stakeholders. Both security and efficiency can be achieved if the public and the responsible authorities adequately understand the issues involved and if there is a proper mix of policies and legislative instruments.⁴⁶⁸

3.2.2.1 Concepts in Oversight

The Commission has concluded that effective oversight in civil aviation security is not possible without a comprehensive regulatory regime. The regime must be made clear to all stakeholders. A thorough assessment of the threat environment and of overall security needs is required before an appropriate regime can be established. Even after it is established, the regime will require constant monitoring and re-evaluation. Oversight will also involve inspection and enforcement efforts to ensure compliance. This will include the regular testing and auditing of security procedures. Transport Canada has a well-developed national network of aviation security inspectors who assess regulatory compliance by CATSA, airports and air carriers,⁴⁶⁹ and who conduct infiltration tests of the security screening system.⁴⁷⁰ Finally, oversight requires Canadian participation and, as appropriate, leadership in international organizations, in particular ICAO. Canada depends in part for its own security on the security regimes of other countries.

3.2.2.2 Oversight of Aviation Security

An adequate regulatory regime and its ongoing review are essential components of oversight in civil aviation security. These are also requirements prescribed by Annex 17 of the *Chicago Convention*. Standard 2.1.2 of the Annex requires each Contracting State to "...establish an organization and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights."⁴⁷¹ Standard 3.1.3 obliges each Contracting State to "...keep under constant review the level of threat to civil aviation within its territory, and establish and implement policies and procedures to adjust relevant elements of its national civil aviation security programme accordingly, based upon a security risk assessment carried out by the relevant national authorities."⁴⁷²

⁴⁶⁷ Exhibit P-169, p. 35 of 202.

⁴⁶⁸ Exhibit P-169, p. 23 of 202.

⁴⁶⁹ Exhibit P-169, p. 87 of 202.

⁴⁷⁰ Exhibit P-173, p. 37.

⁴⁷¹ Exhibit P-181, p. 2-1, s. 2.1.2.

⁴⁷² Exhibit P-181, p. 3-1, s. 3.1.3; see also Exhibit P-169, p. 26 of 202.

In addition, the regulatory regime should ensure that it adequately addresses the particular threat environment facing Canada. The system should account for risks effectively so fewer emergencies arise. At the same time, when emergencies arise, the system should facilitate fully effective crisis management. Any effective security program must be based on reliable intelligence and up-to-date threat assessments, and must be flexible enough to respond to emerging threats.⁴⁷³ Canada does not fully comply with the minimum requirements of Annex 17. It is beyond dispute that many long-recognized risks to civil aviation in Canada have remained inadequately addressed, some for more than 25 years.⁴⁷⁴

3.2.2.2.1 Annex 17 and Canadian Aviation Security

Regulatory Framework

Transport Canada has established regulations, practices and procedures to protect civil aviation from acts of unlawful interference, as required by Standard 2.1.2.⁴⁷⁵ However, it has not ensured that these "...protect the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation," as stipulated by Standard 2.1.3 a) [Emphasis added].⁴⁷⁶ Specifically, Contracting States are obliged under Standard 4.1 to establish measures to prevent unauthorized explosives and other dangerous devices or substances from being introduced on board civil aviation aircraft "by any means whatsoever."⁴⁷⁷ To meet this standard, Contracting States are directed to implement preventive security measures in several areas that:

- Control access to airside and restricted areas of airports,⁴⁷⁸ including the use of identification systems for vehicles entering such areas;⁴⁷⁹
- Protect aircraft,⁴⁸⁰ including the performance of aircraft security checks or searches in certain circumstances;⁴⁸¹
- Screen and protect passengers and baggage;⁴⁸² and
- Subject cargo, mail and other goods to appropriate security controls,⁴⁸³ in the absence of a regulated agent system,⁴⁸⁴ prior to acceptance by passenger aircraft.⁴⁸⁵

⁴⁷³ Exhibit P-169, p. 26 of 202; see also Section 3.4 for a thorough review of the use of intelligence in civil aviation security.

⁴⁷⁴ See Sections 3.8.1, 3.8.2 and 3.8.3, which describe some of the major gaps in the Canadian civil aviation security regime. See also, for example, Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5018-5019.

⁴⁷⁵ Exhibit P-181, p. 2-1, s. 2.1.2.

⁴⁷⁶ Exhibit P-181, p. 2-1, s. 2.1.3 a).

⁴⁷⁷ Exhibit P-181, p. 4-1, s. 4.1.

⁴⁷⁸ See, generally, Exhibit P-181, p. 4-1, s. 4.2.

⁴⁷⁹ See Exhibit P-181, p. 4-1, s. 4.2.3.

⁴⁸⁰ See, generally, Exhibit P-181, p. 4-1, s. 4.3.

⁴⁸¹ Exhibit P-181, p. 4-1, s. 4.3.1.

⁴⁸² See, generally, Exhibit P-181, pp. 4-1–4-2, ss. 4.4 and 4.5.

⁴⁸³ Exhibit P-181, p. 4-2, s. 4.6.

⁴⁸⁴ See Section 3.8.1, which discusses regulated agent systems and the proposed Air Cargo Security Initiative being developed by Transport Canada.

⁴⁸⁵ Exhibit P-181, p. 4-2, s. 4.6.4; see also, in general, Exhibit P-181, p. 4-2, s. 4.6.

The fundamental shortcoming of civil aviation security in Canada is that it is not comprehensive. Security resources have disproportionately focused on passenger and baggage security,⁴⁸⁶ leaving many possible avenues of attack. The civil aviation security system as a whole, which must deal with security issues occasioned by passengers, crew and ground personnel, as well as by the general public, remains vulnerable because it remains possible to place bombs and other weapons of sabotage on aircraft by exploiting air cargo, weaknesses in airport security and other deficiencies.⁴⁸⁷ This situation fails to comply with Standard 4.1.⁴⁸⁸

After the 1985 Air India and 1988 Pan Am bombings and the terrorist attacks of September 11, 2001, significant improvements occurred in Canadian civil aviation security. These dealt primarily with the security screening of passengers and their carry-on and hold baggage.⁴⁸⁹ However, concentrating efforts to improve security almost exclusively on passenger and baggage screening has left other potential routes for sabotage poorly protected or virtually ignored. Specifically, inadequate measures exist to address aspects of airport security,⁴⁹⁰ the security of air cargo, mail and stores,⁴⁹¹ and the security of FBOs and the GA sector.⁴⁹²

There is no evidence that effective identification systems are being used to prevent vehicles from gaining unauthorized access to airside and restricted areas of airports, as required by Standard 4.2.3.⁴⁹³ In fact, there is evidence to the contrary.⁴⁹⁴ The Attorney General of Canada stated that "...vehicles are subject to only cursory, visual examination by airport operators at a limited number of vehicle access gates."⁴⁹⁵ The few security controls that have been applied to air cargo are far from reflecting international best practices⁴⁹⁶ and have not reduced

⁴⁸⁶ Following the events of September 11, 2001, Budget 2001 emphasized passengers as the key risk and directed funding only to passenger transportation. Risks from air cargo and general aviation, for example, attracted less scrutiny, despite the level of concern that has been generated. See Exhibit P-411, pp. 8-9.

⁴⁸⁷ See Sections 3.8.1, 3.8.2 and 3.8.3, which discuss the security risks posed by air cargo, airport security, Fixed Base Operations and the General Aviation sector.

⁴⁸⁸ Standard 4.1 requires Contracting States to establish measures to prevent all dangerous weapons and substances from being introduced on board aircraft engaged in civil aviation "by any means whatsoever." See Exhibit P-181, p. 4-1, s. 4.1.

⁴⁸⁹ See Chapter II and Section 3.1 for a more detailed discussion of the civil aviation security responses to the bombing of Air India Flight 182, the bombing of Pan Am Flight 103 and the attacks of September 11, 2001, respectively.

⁴⁹⁰ See Section 3.8.2, which discusses the deficiencies in airport security.

⁴⁹¹ See Section 3.8.1, which discusses the deficiencies in air cargo security.

⁴⁹² See Section 3.8.3, which discusses the deficiencies in FBO and GA security.

⁴⁹³ Exhibit P-181, p. 4-1, s. 4.2.3.

⁴⁹⁴ In March 2009, a covert operation involving the current Minister of Transport, the Hon. John Baird, and the Chair of the Standing Senate Committee on National Security and Defence, the Hon. Colin Kenny, sought to test airside security at Pearson International Airport in Toronto. The test found that perimeter security was easily breached with a vehicle through an unlocked, unguarded door, and without the need for identification.

⁴⁹⁵ Final Submissions of the Attorney General of Canada, Vol. II, para. 380.

⁴⁹⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4259. See also Section 3.8.1, which discusses the inadequacy of the "known shipper" regime currently in place in Canada and the need for a regulated agent system that is in line with international best practices.

the risk of sabotage through air cargo. They therefore cannot be considered "appropriate security controls,"⁴⁹⁷ as required by Standard 4.6.4.⁴⁹⁸ Transport Canada has acknowledged these security deficiencies, and is considering enhanced security programs for air cargo⁴⁹⁹ as well as for FBOs⁵⁰⁰ and the GA sector.⁵⁰¹ The Department is also currently considering recommendations made by the CATSA Advisory Panel to provide more comprehensive security for airside and restricted areas of airports, including vehicle searches at major airports.⁵⁰²

Canadian aviation security legislative instruments include:

- *Aeronautics Act*;
- *CATSA Act*;
- *Canadian Aviation Security Regulations*;
- *CATSA Aerodrome Designation Regulations*;
- *Designated Provisions Regulations*;
- *Identity Screening Regulations*;
- *Air Carrier Security Measures Order*;
- *Air Carrier Security Measures*;
- *Aerodrome Security Measures Order*;
- *Aerodrome Security Measures*;
- *Security Screening Order*;
- *Special Locations Security Measures*;
- *Civil Aviation Security Alert Condition and Response System for Air Carriers*;
- *Civil Aviation Security Alert Condition and Response System for Aerodrome Operators and Tenants*;
- *Interim Order – Prohibited Items and Prohibited Items List*; and
- *Designation Standards for Screening Officers*.

Some of these instruments are discussed elsewhere in this volume.

National Civil Aviation Security Program and Stakeholder Security Programs

Besides requiring a designated authority responsible for national civil aviation security, Annex 17 sets out several other organizational requirements.⁵⁰³ Key

⁴⁹⁷ Exhibit P-181, p. 4-2, s. 4.6.4.

⁴⁹⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4629. See also Section 3.8.1, which discusses the deficiencies in air cargo security in Canada.

⁴⁹⁹ See Exhibit P-422.

⁵⁰⁰ See Exhibits P-101 CAF0847, CAF0851

⁵⁰¹ See Exhibit P101 CAF0852.

⁵⁰² Exhibit P-101 CAF0871. See also Exhibit P-169, p. 58 of 202.

⁵⁰³ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4271.

among these is an obligation to establish and implement a written national civil aviation security program.⁵⁰⁴ Transport Canada does not have a specific written document that describes the program in its entirety. Rather, the Department states that its substantial body of documents, including all its legislative and regulatory instruments, which together capture all the security requirements, is the equivalent of the national program envisioned by Annex 17.⁵⁰⁵

The experts disagreed with Transport Canada. The CATSA Advisory Panel conceded that Canada likely does comply with the spirit of this Annex 17 requirement, but remained "...convinced that a formal planning system, beginning with Transport Canada, would greatly benefit the aviation security sector."⁵⁰⁶ Wallis did not accept that the legislative and regulatory instruments alone satisfied the Annex 17 requirement for a written national civil aviation security program. He stated that these various documents may contain the vast bulk of information included in a formally written program, but that there was a need for the information to be contained in one document – the format which Annex 17 seems to require.⁵⁰⁷ Although an important guidance document, Canada's National Security Policy, created in 2004,⁵⁰⁸ is not a national civil aviation security program.

There is much evidence to suggest that ICAO expects a single document apart from the legislation that a country develops. First, the confidential ICAO Security Manual provides a sample written national civil aviation security program as guidance about the expectations for such a program.⁵⁰⁹ Second, Wallis suggested that, when interpreting terminology in international civil aviation security conventions, common sense plays a key role.⁵¹⁰ The need to develop and implement regulations, practices and procedures is already addressed in a separate standard of Annex 17.⁵¹¹ Applying a common sense interpretation, a separate standard requiring a written security program implies that something beyond the collection of legislative instruments is necessary. Third, the current Canadian regulatory regime consists of volumes of material. Some stakeholders, particularly air carriers that fly between numerous international jurisdictions, must have a good knowledge of different security regimes to comply with them. Other countries likely have also amassed a considerable volume of legislative and policy instruments.⁵¹² Having all information about security matters in one document – a national civil aviation security program – would make it easier for all stakeholders, policy makers and government officials to understand the program.⁵¹³

504 "Each Contracting State shall establish and implement a written national civil aviation programme to safeguard civil aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights": Exhibit P-181, p. 3-1, s. 3.1.1.

505 Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4791.

506 Exhibit P-169, p. 97 of 202.

507 Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5014.

508 Exhibit P-418.

509 Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5014.

510 Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5000.

511 Exhibit P-181, p. 2-1, s. 2.1.2.

512 Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8211.

513 Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5014.

A separate Annex 17 standard requires the appropriate authority to “define and allocate tasks and coordinate activities” between all entities, including governments, air carriers and airports, that have responsibility for implementing various aspects of the national civil aviation security program.⁵¹⁴ Moses Aléman, an expert in international civil aviation security, discussed the implications of this standard. Reference to the national program, he said, indicated that it must include the state’s full slate of civil aviation security policies and procedures, and must outline each entity’s role so that the functions of all entities were properly coordinated.⁵¹⁵

In fact, Annex 17 requires designated authorities to ensure that airports and air carriers implement and maintain written security programs that conform with the national civil aviation security program.⁵¹⁶ This further suggests the need for a single program document for use as a reference by stakeholders.

Transport Canada no longer requires airports and air carriers to establish written programs.⁵¹⁷ The Department decided during the 1990s to discontinue this obligation. The Department determined that “...a comprehensive program of national regulations that would cover all aspects of aviation security”⁵¹⁸ would suffice and would permit “a uniform national level of security at all airports” to be maintained.⁵¹⁹ The decision to discontinue requiring written security programs was reached only “...after considerable reflection about the most advantageous way of using the security resources available at the time”⁵²⁰ and “...led to the continuing development of a robust program of national aviation security regulations.”⁵²¹

In its 2006 report, the CATSA Advisory Panel recommended that Transport Canada develop a written national civil aviation security program, according to Annex 17 requirements. The Panel further recommended that Transport Canada require airport operators and air carriers to develop and maintain written security programs, and that CATSA and airport tenants do so in their respective areas of responsibility.⁵²² The Panel noted that the UK requires all key stakeholders in civil aviation, including airports, air carriers, cargo shippers and caterers, to produce comprehensive and effective security plans that comply with its national plan. The Panel recommended a similar approach to security

⁵¹⁴ Exhibit P-181, p. 3-1, s. 3.1.4.

⁵¹⁵ Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4272.

⁵¹⁶ Exhibit P-181, p. 3-1, ss. 3.2.1 and 3.3.1.

⁵¹⁷ Exhibit P-169, p. 97 of 202.

⁵¹⁸ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4790.

⁵¹⁹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4790.

⁵²⁰ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4790.

⁵²¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4790.

⁵²² Exhibit P-169, p. 101 of 202.

planning in Canada, particularly as Canada moves towards a more results-based⁵²³ regulatory regime.⁵²⁴

The Commission supports these recommendations of the CATSA Advisory Panel. Clear direction from the governing authority is required in any civil aviation security regime. Formal harmonization of individual security programs within a written national program would show that all stakeholders are working towards the same objectives – an important demonstration that all are “on the same page,” since Canada’s system of enforcement is based upon a philosophy of voluntary compliance, with no monolithic regime imposed from above.⁵²⁵ Transport Canada’s proposed initiative to strengthen air cargo security through a system of regulated shippers, agents and air carriers will require participating entities to submit written security programs with respect to air cargo.⁵²⁶ Transport Canada has indicated that it will consider the CATSA Advisory Panel’s recommendations relating to security programs as part of an initiative to carry out a comprehensive review of its national aviation security regulatory framework.⁵²⁷

In May 2009, Transport Canada announced that the 2009 Budget would include \$2.9 million to support the development of aviation security plans, with the priority being security plans for airports.⁵²⁸

The CATSA Advisory Panel proposed a framework of compulsory security programs that should flow from national transportation and security policies. Besides meeting Annex 17 requirements, a national civil aviation security program would take into account and conform to:

- Canada’s National Security Plan;
- Transport Canada’s National Transportation Policy; and
- Transport Canada’s National Transportation Security Plan.⁵²⁹

A written national civil aviation security program would outline the national policy, as well as the strategy and objectives to be met through a series of integrated industry plans.⁵³⁰

⁵²³ The terms “results-based” and “performance-based” are used interchangeably to describe a regulatory regime in which the outcome is prescribed, but the methods for achieving the outcome remains flexible. This concept is discussed further in Section 3.2.2.2 under the subheading “Underlying Principles.” See also Exhibit P-169, pp. 91-92 of 202.

⁵²⁴ Exhibit P-169, p. 97 of 202.

⁵²⁵ Exhibit P-263, Tab 20, p. 1 of 1.

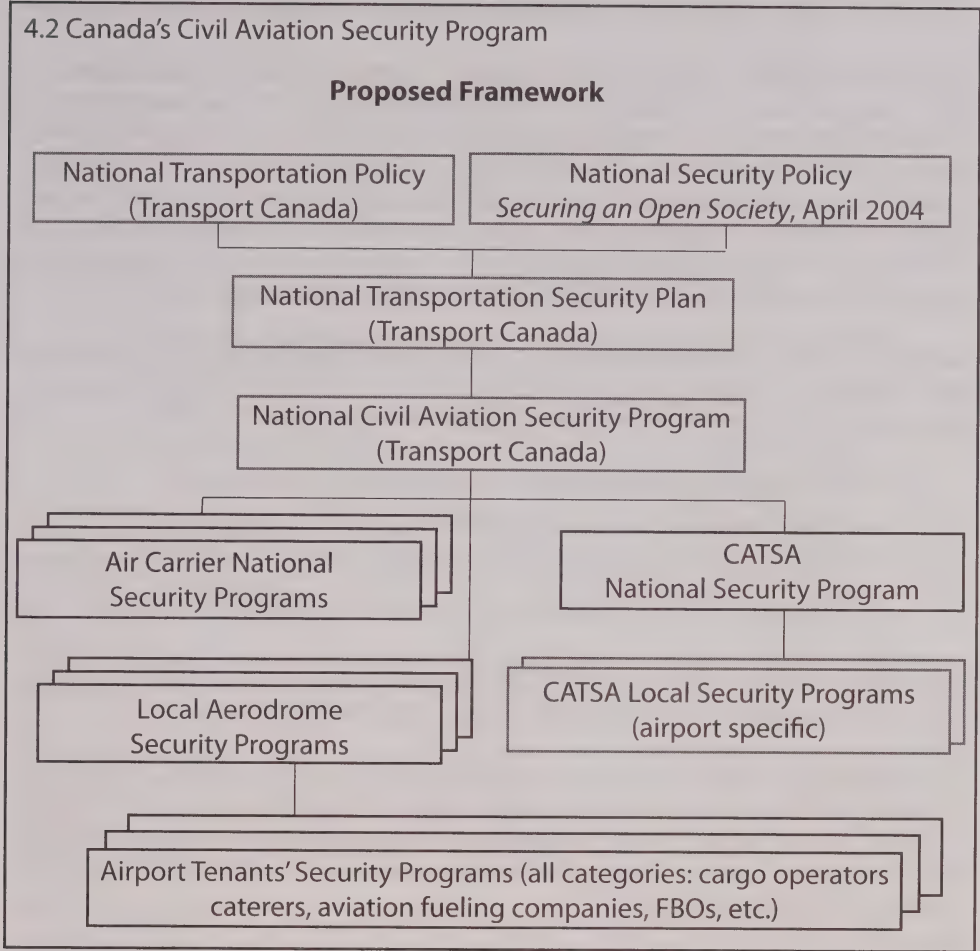
⁵²⁶ Exhibit P-422, pp. 6-8.

⁵²⁷ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4791.

⁵²⁸ Transport Canada News Release, May 5, 2009.

⁵²⁹ Exhibit P-169, p. 98 of 202.

⁵³⁰ Exhibit P-169, p. 98 of 202.

Figure 3: National Civil Aviation Security Program**Exhibit P-169, p. 94**

Within this structure, each major stakeholder would be required to establish security programs that conform to Transport Canada's national civil aviation security program.⁵³¹ As required by Annex 17, Transport Canada would constantly review threat levels and make adjustments to its national civil aviation security program based on risk assessments.⁵³² Similarly, civil aviation stakeholders would undertake a security and risk assessment before establishing their programs, using protocols established by Transport Canada. Although smaller airports would likely have less complex programs and risk assessments than larger ones, the process is "...no less important in maintaining a security posture."⁵³³ Under the proposed structure, CATSA would maintain a national program and

⁵³¹ Exhibit P-169, p. 99 of 202.

⁵³² Exhibit P-181, p. 3-1, s. 3.1.3.

⁵³³ Exhibit P-169, p. 99 of 202.

site-specific programs for all airports at which it operates. These site-specific programs would complement each airport's security program.

Major airport tenants would also be required to produce programs that would form an integral part of each airport's security program.⁵³⁴ As recommended in Transport Canada's proposed Air Cargo Security (ACS) Initiative, all regulated entities, including shippers and freight forwarders located outside the airport, would also be required to submit security programs that correspond to the national program.⁵³⁵ Stakeholder security programs would ideally contribute to meeting the requirement to have a national civil aviation security program by clearly defining the responsibilities and authority of each organization.

Aviation security programs would identify weaknesses in infrastructure, policies and procedures, as well as the potential countermeasures and changes that may be required. At a minimum, programs would include:

- Measures to prevent unauthorized access to facilities;
- Assignment of security-related duties and responsibilities;
- Procedures for responding to threats to or breaches of security; and
- Procedures for periodically reviewing and updating programs.⁵³⁶

Programs would include a description of how entities meet regulated objectives, with periodic auditing by Transport Canada inspectors.

In its oversight capacity, Transport Canada would approve programs and ensure compliance through monitoring and enforcement.⁵³⁷ Multi-year programs could be approved and adjusted as necessary.⁵³⁸ This integrated system of security programs would be similar to the regime that was established for marine security after September 2001.⁵³⁹

National Aviation Security Committee and Stakeholder Security Committees

Annex 17 also contains a requirement for stakeholder collaboration. Standard 3.1.5 requires Contracting States to establish a national aviation security committee "...for the purpose of coordinating security activities" between government departments and agencies, airport and aircraft operators and others responsible for implementing aspects of the national civil aviation

⁵³⁴ Exhibit P-169, p. 99 of 202.

⁵³⁵ Exhibit P-422, pp. 6-8.

⁵³⁶ Exhibit P-169, p. 99 of 202.

⁵³⁷ Exhibit P-169, p. 99 of 202.

⁵³⁸ Exhibit P-169, p. 99 of 202.

⁵³⁹ The system for marine security was implemented under the *Marine Transportation Security Act* and the *Marine Transportation Security Regulations*. See Exhibit P-169, p. 99 of 202.

security program.⁵⁴⁰ In 2005, Transport Canada established the Advisory Group on Aviation Security (AGAS), which appears to serve a similar purpose.

The AGAS plays an important consultative role at the national level, bringing together government and aviation industry representatives twice yearly⁵⁴¹ to exchange views on aviation security policy, strategy and regulatory and program priorities.⁵⁴² It is a forum for high-level discussions between senior levels within federal departments and the Canadian aviation security community.⁵⁴³ AGAS meetings consist of:

- Security intelligence briefings;
- Transport Canada briefings on aviation security policy and on regulatory and program priorities;
- High-level strategic advice from stakeholders;
- Discussion of common problems to determine whether the program is appropriate for the threat and risk environment; and
- Progress reports from technical committees, including those dealing with air carrier security, aerodrome security and security screening.⁵⁴⁴

Annex 17 also requires each airport to establish an airport security committee to assist in implementing the airport security program.⁵⁴⁵ The *Canadian Aviation Security Regulations* require airports to have security committees, but these committees vary in size, level of representation and effectiveness. The CATSA Advisory Panel called for a more consistent approach to ensure the systematic sharing of information among committee members and a solid foundation for establishing common goals and procedures in aviation security incidents.⁵⁴⁶

Security programs and committees are essential to ensure optimal communication among those responsible for civil aviation security.⁵⁴⁷ Wallis argued that ongoing, open dialogue between government officials, who often do not possess practical, on-the-ground experience in aviation security, and representatives of airports and air carriers, as well as others involved in ensuring

⁵⁴⁰ “Each Contracting State shall establish a national aviation security committee or similar arrangements for the purpose of coordinating security activities between the departments, agencies and other organizations of the State, airport and aircraft operators and other entities concerned with or responsible for the implementation of various aspects of the national civil aviation security programme”: Exhibit P-181, p. 3-1, s. 3.1.5.

⁵⁴¹ Exhibit P-101 CAF0859, p. 3 of 44.

⁵⁴² Participants in AGAS include representatives of airport authorities, air carriers, police departments, courier services, relevant Transport Canada departments, industry associations, CATSA, IATA, labour groups and cargo carriers. See Exhibit P-101 CAF0860 for a list of participants; see also Exhibit P-169, p. 49 of 202.

⁵⁴³ Exhibit P-101 CAF0859, p. 3 of 44.

⁵⁴⁴ Exhibit P-101 CAF0859, pp. 2-3 of 44.

⁵⁴⁵ Exhibit P-181, p. 3-1, s. 3.2.3.

⁵⁴⁶ Exhibit P-169, p. 49 of 202.

⁵⁴⁷ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4271.

the security of civil aviation, is important for developing sound security measures and procedures for the industry.⁵⁴⁸

3.2.2.2 Regulatory Regime

Underlying Principles

A sufficiently robust regime can be achieved and sustained through adherence to several key principles repeatedly mentioned by many experts and stakeholders who appeared before the Commission. These principles include the following:

- Developing measures in a proactive manner;
- Establishing a multi-layered system of security;⁵⁴⁹
- Providing for flexibility and performance-based measures, where suitable;⁵⁵⁰
- Fostering a culture of security awareness; and
- Determining the relative need for security measures through the systematic application of accepted risk management protocols, both on an individual and on a global basis.⁵⁵¹

The effectiveness of the regime in confronting past, present and future threats must be constantly scrutinized.

These principles are all aimed at achieving civil aviation security's ultimate objective – prevention.

Proactive Approach

A proactive approach is critical in civil aviation security, since the ultimate goal is to anticipate and thwart unlawful interference.⁵⁵² Yet this approach has been largely missing in Canada and throughout the world. Canadian security, like security in other jurisdictions, has generally been reactive. Dr. Reg Whitaker, Chair of the CATSA Advisory Panel, elaborated:

We noticed very clearly the reactive quality of Canadian security. The pattern is recurrent. It is always plugging the holes that have appeared. We have had – if you [go] back to the pre-Air India [bombing] era, the focus on airline hijacking and the concern to prevent hijacking, [which was] perfectly reasonable but it focused attention in a certain direction and then suddenly you had a bomb being put on a plane unaccompanied by a passenger.

⁵⁴⁸ Wallis, *Combating Air Terrorism*, p. 37.

⁵⁴⁹ Exhibit P-169, p. 38 of 202.

⁵⁵⁰ Exhibit P-169, pp. 92-93 of 202.

⁵⁵¹ Exhibit P-361, Tab 1, p.10; See Section 3.3.

⁵⁵² Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8114.

And then in the aftermath of Air India, we had, again, reasonable and important responses to that such as passenger baggage reconciliation, but again a kind of pattern of looking backward after 9/11, and the sudden appearance of the idea of the suicide terrorist using a plane as a weapon and then we have a whole new set of responses.

All these are necessary, certainly, but there is a danger that we are always, to use a particular metaphor I suppose, fighting the last war instead of the next. This is easy to say, but it is much harder to come to [a] determination of how...[to] develop the capacity to think ahead, to be imaginative, to anticipate a threat which is in fact a constantly evolving threat. Terrorists don't stand still and they analyze the kind of security that we have and think of ways of getting around it and think of imaginative ways, as happened in 9/11, of inflicting terror.⁵⁵³

The Panel acknowledged that applying a proactive approach in practice is inherently challenging.⁵⁵⁴ Dr. Jacques Bourgault, a member of the Panel, stressed that proactive thinking must not occur sporadically. Rather, it must be part of the overall strategic plan, with organizations taking a proactive approach on a continuous basis.⁵⁵⁵ However, noted Bourgault, history has demonstrated that the desired approach is not always achieved:

The experience has proven that looking forward is not part of the usual practices, not only in Canada, in most of the countries, and it's a problem because from time to time, terrorists win, as we have seen.⁵⁵⁶

The Hon. Bob Rae also discussed both the challenges and importance of implementing a proactive approach in civil aviation security:

...[I]t is very hard to predict where the next threat is going to come from or where it may take place. It's very, very difficult for us to know that. So all you can do is have a series of contingencies which allow you to do [that].

I am reminded of the phrase which emerged from 9/11 which was that 9/11 – the question was not that it was a failure of intelligence but it was a failure of imagination and I think that is where one hopes that government would have an

⁵⁵³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4646.

⁵⁵⁴ See Testimony of Reg Whitaker, Chern Heed and Jacques Bourgault, vol. 38, June 1, 2007, p. 4647.

⁵⁵⁵ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4647.

⁵⁵⁶ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4648.

ability to imagine things that might happen and what are the contingencies that should be put in place to deal with those terrible possibilities, and that is what I think we should be spending some time as a country thinking about.⁵⁵⁷

Layered Approach

The Commission heard repeatedly that a multi-layered approach to civil aviation security is essential. Since no procedure or measure is foolproof,⁵⁵⁸ a system of redundancies is necessary, so that if a terrorist penetrates one layer of security, protection is still provided by the remaining layers.⁵⁵⁹ Analogies were made to layers of an onion: if one layer is peeled away, another is revealed beneath it. Comparison was also made to a “Swiss cheese” model, in which each layer of security has holes, or areas of weakness, but as long as the layers are positioned to ensure that the holes do not line up, security is maintained.⁵⁶⁰

Canada advocates, but does not achieve in practice, a multi-layered system of security in which mutually reinforcing and complementary layers ensure “... that when passengers and baggage get on board aircraft they are as secure as they can be.”⁵⁶¹ The layered approach can be applied to a specific security measure, such as the multi-tiered process for hold bag screening (HBS), where checked baggage can pass through up to five levels of screening before being cleared for loading onto an aircraft. This process recognizes that no one piece of equipment or method of screening baggage is fail-safe. The concept of layering also applies to the aviation security system as a whole. Organizations and authorities, each with specific security responsibilities, have been established, along with accompanying security measures, to address all vulnerabilities.⁵⁶²

Performance-based Approach

A performance-based (also known as “results-based”)⁵⁶³ approach prescribes the desired outcome, but does not dictate how to achieve it. This approach recognizes that resources and facilities differ among those responsible for security and that, as long as the objective is achieved, the precise method becomes less important. For example, a performance-based approach recognizes that several electronic and manual methods are available to ensure that an unaccompanied bag does not travel if the corresponding passenger is not on board the flight. The exact method can be left to the air carrier. This approach differs from the prescriptive approach imposed for passenger-baggage reconciliation after the Air India bombings.

⁵⁵⁷ Testimony of Bob Rae, vol. 58, October 4, 2006, p. 567.

⁵⁵⁸ Wallis, *How Safe Are Our Skies?*, p. 81.

⁵⁵⁹ Exhibit P-169, p. 38 of 202; see also Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4637.

⁵⁶⁰ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7933.

⁵⁶¹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4708.

⁵⁶² Exhibit P-169, pp. 38-39 of 202.

⁵⁶³ Exhibit P-169, p. 91 of 202.

The terrorist threat is constantly evolving. The Commission heard that a more flexible, performance-based, regulatory approach to security is necessary as a result. After the Air India bombing, Transport Canada moved from a “planning and performance-based regulatory framework”⁵⁶⁴ to a more prescriptive regulatory framework, which involved detailed regulations for procedures such as passenger-baggage reconciliation.⁵⁶⁵ Whitaker stated that this was an appropriate response at the time, given the egregious security breaches exposed by the bombing.⁵⁶⁶ Before 1985, responsibility for screening was left to air carriers, whose focus on customer service resulted in security not being a priority.⁵⁶⁷ Air carriers were required to submit their security programs to Transport Canada, but no formal approval process was set out in legislation. The CATSA Advisory Panel concluded that the regime at the time was vague and had left “a degree of interpretation and flexibility”⁵⁶⁸ about how air carriers designed and implemented their security systems. The 1985 Seaborn Report, which reviewed airport and airline security following the Air India bombings, understandably recommended a more prescriptive aviation security regime.⁵⁶⁹ This prescriptive approach was reinforced after the September 11, 2001, attacks when authorities further tightened the rules.⁵⁷⁰

However, the CATSA Advisory Panel concluded that an overly prescriptive regulatory framework might reduce security. Rigid procedures could become predictable, enabling someone who observed the system over time to circumvent it. An inability to adopt new equipment and security methods quickly might also reduce security. In certain circumstances, rigidity would simply increase costs and reduce security.⁵⁷¹

For example, the Panel noted that the *Security Screening Order* which, together with the *Canadian Aviation Security Regulations*, defined CATSA’s roles and responsibilities, left little room for CATSA to make operational decisions, deploy resources efficiently or develop new ways to achieve its objectives. CATSA’s inability to deviate from the regulations and security orders sometimes reduced both service to customers and cost effectiveness.⁵⁷²

CATSA itself called for increased financial flexibility in its operations.⁵⁷³ During the liquid and gel explosives threat in August 2006, CATSA required extra funds for a public awareness campaign.⁵⁷⁴ Crown corporations would normally set their own operational policy, but CATSA’s ability to do so was largely dictated by the regulatory framework. The Panel observed that this framework did not provide

⁵⁶⁴ Exhibit P-169, p. 91 of 202.

⁵⁶⁵ Exhibit P-169, p. 91 of 202.

⁵⁶⁶ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4624.

⁵⁶⁷ Exhibit P-169, p. 92 of 202.

⁵⁶⁸ Exhibit P-157, pp. 19-20 of 135.

⁵⁶⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4624.

⁵⁷⁰ Exhibit P-169, p. 91 of 202.

⁵⁷¹ Exhibit P-169, p. 91 of 202.

⁵⁷² Exhibit P-169, p. 91 of 202.

⁵⁷³ Exhibit P-101 CAF0827, p. 2 of 19.

⁵⁷⁴ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4843.

for "...the managerial discretion and creativity necessary to achieve its other objectives in a balanced way."⁵⁷⁵ The Panel contended that CATSA had reached a level of maturity as an organization because it possessed the experience and knowledge to make operational decisions and to be held accountable for them, provided that security remained its main focus.⁵⁷⁶

Many industry stakeholders stressed to the Commission the importance of avoiding a "one-size-fits-all" approach to aviation security.⁵⁷⁷ Stephen Conrad, Project Director for Air Cargo Security at Transport Canada, testified that both prescriptive and performance-based measures might be required, depending on the context. Where a measure was very technical or complex, a greater degree of prescription might be warranted.⁵⁷⁸

The CATSA Advisory Panel also acknowledged that "...[r]egulation, ranging from prescriptive to results-based, has to be seen as a continuum rather than a dichotomy"⁵⁷⁹ and that some prescription would always be required for security matters.⁵⁸⁰ However, the Panel concluded that, with a much better aviation security regime in place today than in 1985, and with a Crown Corporation, rather than air carriers, now responsible for screening, the regime imposed on CATSA was too heavily weighted towards prescription. It also concluded that the private sector would benefit from a performance-based approach to aviation security. Bourgault testified that "...CATSA, with...[its] operational procedures, has to be prescriptive with its own personnel doing the searching. But CATSA as a body, as a corporation, has to be results-based in terms of procedures, protocols and approach to prevent any terrorist attack."⁵⁸¹

Transport Canada favours a more performance-based approach to aviation security. It recently initiated a multi-year and comprehensive review of Canada's aviation security regulatory framework.

The CATSA Advisory Panel stated that performance-based regulations could be either "loosely" or "tightly" specified. A somewhat tighter approach might be appropriate for industry, in part because of its profit motive and tendency to contain costs. For a government agency such as CATSA, whose entire purpose was security, the Panel suggested a looser approach.⁵⁸²

Conrad testified that the flexibility afforded by a performance-based approach enabled industry and other stakeholders to devise "unique and innovative

⁵⁷⁵ Exhibit P-169, p. 90 of 202.

⁵⁷⁶ Exhibit P-169, pp. 91-92 of 202.

⁵⁷⁷ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8114; see also Exhibit P-101 CAF0827, p. 16 of 19.

⁵⁷⁸ Conrad spoke particularly in the context of a proposed Air Cargo Security (ACS) Initiative that would see security controls applied to air cargo by industry outside the air terminal building: Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5185-5186.

⁵⁷⁹ Exhibit P-169, p. 93 of 202.

⁵⁸⁰ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4625.

⁵⁸¹ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4625.

⁵⁸² Exhibit P-169, p. 95 of 202.

ways of solving new and emerging problems”⁵⁸³ and to meet their compliance obligations in the most efficient and cost-effective manner. The CATSA Advisory Panel concluded that this approach also facilitated a culture of continuous improvement, a characteristic of a “high reliability organization.”⁵⁸⁴ It was also a typical objective in risk management.⁵⁸⁵

The Panel concluded that, for regulators, performance-based requirements were simpler and less detailed to prepare in the first instance. This reduced the need for regulatory exemptions and the time and effort required to produce regulatory amendments. This would free Transport Canada from making and enforcing detailed rules, enabling it to focus on other pressing objectives, such as the development of an air cargo security regime.

The Panel described the disadvantages of the performance-based approach as including greater complexity in compliance monitoring than under the prescriptive approach. The Panel stated that a performance-based regime required a culture shift by inspectors to an audit approach to compliance monitoring, but that this should allow for more efficient use of inspectors. A performance-based approach might also make it more difficult for a regulator to demonstrate compliance with international agreements. The Panel noted that a performance-based regime could be supported by a Security Management Systems (SeMS) approach (discussed below), with which international bodies such as ICAO and many ICAO member states were familiar. SeMS was being actively discussed in these venues.⁵⁸⁶

The Panel warned, however, that with any move towards a performance-based regime, Transport Canada must still fulfill its obligations under Annex 17. In particular, Transport Canada needed to develop a written national civil aviation security program and require all stakeholders to develop programs for their operations that are consistent with the national plan. Compliance with the approved programs would then be monitored and audited through regular inspections by Transport Canada.⁵⁸⁷ The Panel called for AGAS, which plays an important consultative role at the national level by bringing together government and industry participants, to be fully engaged in the development and maintenance of a performance-based regime.⁵⁸⁸

From January to April 2008, Transport Canada held briefings with industry stakeholders to explain an aviation security regulatory review that was designed to enhance and update the regulatory framework.⁵⁸⁹ Stakeholders stressed the need for clarity about government and industry responsibilities.⁵⁹⁰ This was an

⁵⁸³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5186.

⁵⁸⁴ Exhibit P-169, p. 95 of 202.

⁵⁸⁵ Exhibit P-361, Tab 1, p. 10.

⁵⁸⁶ Exhibit P-169, p. 95 of 202.

⁵⁸⁷ Testimony of Reg Whitaker and Chern Heed, vol. 38, June 1, 2007, pp. 4625-4626.

⁵⁸⁸ Exhibit P-169, pp. 95-96 of 202.

⁵⁸⁹ Exhibit P-101 CAF0827, p. 16 of 19.

⁵⁹⁰ Exhibit P-101 CAF0827, p. 16 of 19.

important point. The Fatal Accident Inquiry in Scotland, which reviewed the bombing of Pan Am Flight 103, found that the directions and circulars issued by the UK Department of Transport were not sufficient to ensure that an “infiltrated” unaccompanied bag would not be placed on board the flight when a transfer of aircraft took place at Heathrow Airport.⁵⁹¹ Writing in 1993, Wallis stated that this finding was highly significant⁵⁹²:

Many government civil aviation officials around the world have been apt to issue directives with little or no effort being made to ensure their terms are understood. Monitoring implementation of the regulations is frequently nonexistent. Often the rules are put together by civil servants who have no practical experience of airline or airport operations and are developed without consultation with aviation operations executives.... Rules laid down by a state’s aviation authorities should be crystal clear to all parties.⁵⁹³

The CATSA Advisory Panel recommended that Transport Canada make it a “high priority” to develop a more results-based regulatory framework for aviation security.⁵⁹⁴

Any move to a performance-based regulatory regime must involve effective, clear communication between all organizations with responsibilities in civil aviation security, as well as vigilant oversight by Transport Canada. Where measures are performance-based, the outcome prescribed should specify the highest possible standard, based on risk management principles. Care must be taken to avoid crafting “minimum standards” like those in the Annex 17 provisions.

Security Culture and Risk Management⁵⁹⁵

Absolute security is not achievable.⁵⁹⁶ However, optimal security can be obtained through proper risk management, which seeks to find the most cost-effective ways to allocate limited resources for dealing with each risk. Risk management protocols provide a systematic approach for reviewing a global set of risks, which are then prioritized and addressed so that all significant risks are reduced to an acceptable level. Since responsibility for civil aviation security is divided among several industry, government and non-profit organizations, common protocols and a shared understanding for carrying out risk assessment and risk management procedures are essential. Rigorous risk management principles must be an integral component of any civil aviation security system.⁵⁹⁷

⁵⁹¹ Wallis, *Combating Air Terrorism*, p. 36.

⁵⁹² Wallis, *Combating Air Terrorism*, p. 37.

⁵⁹³ Wallis, *Combating Air Terrorism*, p. 37.

⁵⁹⁴ Exhibit P-169, p. 93 of 202.

⁵⁹⁵ See Section 3.3.7, which also discusses the establishment of a security culture.

⁵⁹⁶ See, for example, Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8148; see also Exhibit P-169, p. 36 of 202.

⁵⁹⁷ Exhibit P-361, Tab 1, pp. 8-10.

The Commission notes the holistic approach to risk management adopted by Australia and New Zealand. Their national risk management standards encourage risk management processes to be integrated into an organization's philosophy and practices, rather than being viewed as a separate activity, so that "...everyone in the organization becomes involved in the management of risk."⁵⁹⁸

The CATSA Advisory Panel recommended Security Management Systems (SeMS) as the methodology that could best support a performance-based regime.⁵⁹⁹ SeMS has been described as an approach that incorporates many of the key underlying principles needed to ensure a robust civil aviation security regime, including increased operational flexibility, a proactive approach and a rigorous risk management process that prioritizes risks and addresses them in a timely and preventive manner.⁶⁰⁰

The Commission learned that the concept for SeMS was derived from a model developed to address issues related to aviation safety, known as safety management systems, which was being implemented by airports, air carriers and other stakeholders in the aviation system at the time of the hearings.⁶⁰¹ One reported strength of the safety management systems approach is its practice of non-punitive reporting of safety concerns, in which all involved are encouraged to report potential problems without fear of retribution. The entire thrust is accident prevention.⁶⁰² The safety management systems approach is expected to produce a lower accident rate through more proactive management of risk, reduced industry costs and more efficient use of government resources, all of which would benefit security as well.⁶⁰³

SeMS adopts the core principles of the safety management systems approach, extending them to the security environment for application by airports, air carriers, CATSA and others with responsibilities in aviation security. Some of the more significant elements of this approach include timely sharing of information, a culture of greater security awareness, reporting of potential hazards and self-auditing of security programs.⁶⁰⁴ The CATSA Advisory Panel described how to employ the SeMS approach:

To be effective, SeMS must become an element of corporate management that sets out the organization's security policies and its intent to embrace security as an integral part of its overall business. Thus, security becomes a culture that percolates throughout the entire organization rather than simply being an obligation. There are various basic

⁵⁹⁸ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 12.

⁵⁹⁹ Exhibit P-169, p. 93 of 202.

⁶⁰⁰ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8114.

⁶⁰¹ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8113-8114.

⁶⁰² Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8000.

⁶⁰³ Exhibit P-169, p. 94 of 202.

⁶⁰⁴ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8113-8114.

elements associated with SeMS, including adopting a security management plan, implementing a training program, tracking quality assurance and oversight, as well as developing an emergency response plan.⁶⁰⁵

Although many industry stakeholders indicated their support for SeMS, the Commission was informed that the concept was still under development.⁶⁰⁶ In May 2008, Transport Canada gave the Commission a discussion paper describing the conceptual framework for SeMS. This was Transport Canada's most current document on the topic, but officials advised that its contents were likely outdated, as thinking around SeMS had evolved since January 2007, when the paper was produced.⁶⁰⁷ Some industry stakeholders were confused about the meaning of SeMS and how it was to be applied.⁶⁰⁸ Concerns were also expressed about the effective application of the principles of safety management systems to the security environment, since issues of safety deal with unintended actions, whereas security must prevent intentional harm.⁶⁰⁹

As part of the consultative process provided by AGAS, a SeMS technical committee was established to develop the details of the regulatory structure for SeMS, with input from civil aviation stakeholders.⁶¹⁰ Fred Jones, Vice President Operations and Legal Affairs with the Canadian Airports Council (CAC), which was involved in this process, told the Commission that "...right now we're talking about principles; we'd like to reduce them to...more concrete practices on a national level."⁶¹¹

Transport Canada also advised that industry, CATSA and other key stakeholders were being consulted "...to answer broad and fundamental questions still outstanding for policy and implementation,"⁶¹² and that it had sought the input and expertise of international stakeholders, including the G8, ICAO, IATA and the DHS,⁶¹³ to identify best practices in the field.⁶¹⁴ It noted growing government and industry interest in SeMS. Some industry organizations, such as IATA, were actively pursuing a SeMS approach.⁶¹⁵ Transport Canada reported that the SeMS approach was a strategic priority and key element of its vision for securing Canada's transportation system:

A SeMS approach will focus regulators and industry on achieving strong levels of security performance in areas of

⁶⁰⁵ Exhibit P-169, p. 93 of 202.

⁶⁰⁶ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8114.

⁶⁰⁷ Exhibit P-101 CAF0827, p. 10 of 19.

⁶⁰⁸ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8000.

⁶⁰⁹ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8000.

⁶¹⁰ Testimony of Fred Jones, vol. 64, October 24, 2007, p. 8114.

⁶¹¹ Testimony of Fred Jones, vol. 64, October 24, 2007, p. 8114.

⁶¹² Exhibit P-101 CAF0835, p. 17 of 35.

⁶¹³ Exhibit P-101 CAF0835, p. 17 of 35.

⁶¹⁴ Exhibit P-101 CAF0837, p. 1 of 1.

⁶¹⁵ Exhibit P-101 CAF0837, p. 1 of 1.

highest security risk and priority. It does not replace other regulatory requirements, but builds upon them while moving TC [Transport Canada] and industry to an approach that is more proactive, collaborative, performance-based, and incorporates risk-management principles.⁶¹⁶

The Commission encourages further discussion and development of SeMS through the consultative process of AGAS but, as discussed elsewhere,⁶¹⁷ it remains cautious about broad concepts that may be poorly understood. There is no doubt that a culture of greater security awareness is imperative for the current security regime. However, any system-wide approach requires clarity, precision in terminology and a solid understanding among stakeholders of what is required of each of them. As well, greater responsibilities for other players in civil aviation should not absolve Transport Canada of its overall responsibilities as regulator.

Identifying Threats: Past, Present and Future

A thorough grasp of the historical developments relating to unlawful interference with civil aviation is a vital part of Transport Canada's oversight role, and is consistent with its duty to build an appropriate regulatory regime for civil aviation security. As well, Transport Canada must constantly monitor global incidents and trends, however insignificant they may at first seem. Dr. Peter St. John, a retired professor of international relations with expertise in air terrorism, testified that it is only through persistent attention that patterns emerge and connections can be made that may assist in revealing threats – from the past, present and into the future – that might otherwise pass unnoticed.⁶¹⁸ Wallis contended that the isolationist stance in North America should have come to an end with the bombing of Air India Flight 182 in 1985, which demonstrated that terrorism was not confined to other parts of the world. Ongoing critical analysis of threats in the Canadian context is required. This may seem an obvious prerequisite for oversight responsibilities in civil aviation security, and an exercise that must be conducted in any analysis of risk,⁶¹⁹ but the record to date fails to show that this ongoing analysis has occurred in Canada or beyond. The importance of such analysis cannot be overstated:

Review of past incidents is vital if aviation security is to close the door to terrorists. But the task in this millennium must be for security executives to be proactive rather than reactive. For this to happen, the right people have to be employed to direct the security functions within airlines, at airports, and within

⁶¹⁶ Exhibit P-101 CAF0837, p. 1 of 1.

⁶¹⁷ See Section 3.3.7.

⁶¹⁸ See Testimony of Peter St. John, vol. 35, May 29, 2007, pp. 4220-4223.

⁶¹⁹ Formal risk management procedures in civil aviation security were only recently introduced by Transport Canada in 2006, and some concerns have been expressed about the comprehensiveness of the process. For a more detailed analysis, see Section 3.3.4.

governments. Security directors, whether within an airline or with an airport company, must meet the needs of the task delegated to them. Good aviation security depends on the caliber, the knowledge, and the experience of the personnel selected to manage the function.⁶²⁰

Since the early days of air terrorism, measures for safeguarding civil aviation have been largely unplanned, responding to incidents as they occurred, rather than being produced in an anticipatory, proactive manner. The continuing reactive stance seen at the international level has been mirrored domestically.⁶²¹ But a cursory study of past acts of unlawful interference reveals several incidents where terrorist tactics provoked no new security measures. The same tactics were used later, ostensibly taking the civil aviation community by surprise.

Rae described the failure to anticipate the terrorist attacks of September 11, 2001 as a failure of imagination.⁶²² Almost 30 years earlier, in 1972, hijackers of Southern Airways Flight 49 in the US threatened to crash the plane into an atomic power plant in Tennessee, presaging the use of aircraft as weapons in themselves.⁶²³ In 1987, all 115 on board Korean Airlines Flight 858 were killed after it was destroyed as it flew over the Andaman Sea. Liquid explosives had been deliberately carried on board by passengers belonging to the North Korean Workers Party.⁶²⁴ Still, the civil aviation security community did not address the threat from liquid explosives until 2006, when a plot to use liquid and gel explosives against several aircraft leaving the UK was unearthed. Only then were measures introduced to restrict liquids and gels in carry-on luggage, first in the form of hasty emergency measures and later, as the immediate threat subsided, as a standard part of pre-board screening (PBS).

St. John testified that a careful examination of past acts of unlawful interference with civil aviation revealed a number of patterns. Since 1947, there had been five or six “cycles” of civil aviation incidents. This indicated a certain predictability and therefore had implications for assessing threats to the system. He said that the copycat effect, for example, was prevalent in aviation terrorism: “Ideas that are in the air are captured and used and reused by successive people.”⁶²⁵

Wallis also spoke of the importance of looking at past incidents:

⁶²⁰ Wallis, *How Safe Are Our Skies?*, p. 165.

⁶²¹ See Chapter II and Section 3.1, which detail the specific enhancements to the civil aviation security regime following the bombing of Air India Flight 182, the bombing of Pan Am Flight 103 and the terrorist attacks of September 11, 2001, respectively.

⁶²² Testimony of Bob Rae, vol. 58, October 4, 2006, p. 567.

⁶²³ This was a lengthy hijacking in which the aircraft landed at several locations in North America, including Toronto and twice in Cuba, before the incident was resolved. See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

⁶²⁴ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

⁶²⁵ Testimony of Peter St. John, vol. 35, May 29, 2007, p. 4222.

Hindsight is a great blessing. History provides an opportunity for turning hindsight into foresight. Hands-on experience gained in a variety of countries helps in the development of security defences. All security executives should have this experience and be avid students of what has gone on before. It will help them predict and prevent incidents occurring in the future. It will also go a long way to making the skies safer for passengers and crews and for people on the ground. Security managers must always be open to innovative ideas and be unafraid to experiment in the interest of passenger security.⁶²⁶

3.2.2.2.3 *Inspection and Enforcement*

In carrying out oversight, Transport Canada has established a system for inspection and enforcement of the national regulatory regime, which includes the *Aeronautics Act* and the *CATSA Act*, regulations, measures and orders. At the larger airports, inspectors are kept on site. Smaller airports are subject to regular visits by inspectors. Inspectors perform oversight of airport, air carrier and CATSA operations.⁶²⁷

There are approximately 120 inspectors in Canada, posted across five regions. They are responsible for providing a constant or occasional presence at the 89 “designated” airports, depending on the airport category. Inspectors perform duties related to Canada’s Aviation Security Inspection and Enforcement Program. The key components of the program are prevention, detection, investigation and enforcement.⁶²⁸

Prevention activities are conducted through education, presence, advertising and consulting. The objectives are to prevent violations and to promote voluntary compliance. Detection activities include observation, monitoring, inspection, auditing and testing against legislation to determine whether aerodromes, air carriers and screening authorities are in compliance. This includes infiltration tests of screening checkpoints, hold baggage screening, cargo facilities, Restricted Area Identification Cards and aircraft security. A rigid protocol for infiltration tests is laid out in the Inspection and Enforcement Manual.⁶²⁹ Infiltration testing is a key component of compliance monitoring.⁶³⁰

Investigations attempt to determine whether a contravention has occurred and, if so, whether reasonable grounds exist for enforcement action. Enforcement action could include verbal warnings, letters of enforcement and “administrative

⁶²⁶ Wallis, *How Safe Are Our Skies?*, p. 166.

⁶²⁷ Exhibit P-169, p. 87 of 202.

⁶²⁸ Exhibit P-101 CAF0827, p. 15 of 19.

⁶²⁹ The Inspection and Enforcement Manual was presented to the Commission in November 2007.

⁶³⁰ Exhibit P-101 CAF0827, p. 15 of 19.

monetary penalties” under the *Aeronautics Act*. No criminal penalties are involved. Inspectors are responsible for verifying that deficiencies are corrected.⁶³¹

The overall approach is one of voluntary compliance,⁶³² with a formal policy requiring such compliance developed after the bombing of Air India Flight 182.⁶³³ Transport Canada’s philosophy of voluntary compliance is governed by principles including transparency, fairness, timeliness, consistency and confidentiality.⁶³⁴ Although voluntary compliance is encouraged through an incremental approach to enforcement, earlier imposition of the more severe penalties for non-compliance may sometimes be warranted.

Inspections are also conducted to ensure that relevant overseas operations comply with Canadian requirements. As part of the Off-shore Inspection Security Program, teams of security specialists are sent to inspect foreign air carrier operations in other countries to verify compliance with Canada’s regulatory regime. Before issuing operating certificates to foreign air carriers, Canadian inspectors visit the off-shore site to ensure that standard bilateral reciprocal security clauses will be honoured. Such clauses form part of bilateral agreements with foreign air carriers and stipulate that Annex 17 standards and Canadian regulatory requirements will be respected.⁶³⁵

Inspectors are trained over an 18-month period, and their powers are granted incrementally. Inspectors must satisfy a test of competence at each level of their training.⁶³⁶

3.2.2.2.4 Shared Responsibility: Role of Stakeholders in Oversight

Stakeholders also have to perform oversight of their own security operations. For example, Yves Duguay, Director of Security for Air Canada at the time of the Commission hearings, testified that Air Canada tested its aircraft groomers and cleaners by hiding prohibited items on an aircraft to see if they were discovered. If the items were not found, issues of compliance and security awareness were addressed. Air Canada developed this testing based on the best practices being used by Transport Canada. Air Canada also tested other security procedures for which it was responsible, including passenger-baggage reconciliation and intrusions into restricted areas.⁶³⁷

In its review of the Canadian aviation security regime, the CATSA Advisory Panel expressed concerns about the overlapping and potentially excessive oversight brought to bear on security screening personnel,⁶³⁸ confusion about which rules

⁶³¹ Exhibit P-101 CAF0827, p. 16 of 19.

⁶³² Exhibit P-101 CAF0827, p. 16 of 19.

⁶³³ Exhibit P-263, Tab 15, p. 3 of 5.

⁶³⁴ Exhibit P-263, Tab 20, p. 1 of 1.

⁶³⁵ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4541.

⁶³⁶ Exhibit P-101 CAF0827, p. 16 of 19.

⁶³⁷ Testimony of Yves Duguay, June 14, 2007, p. 5269.

⁶³⁸ Exhibit P-169, p. 87 of 202.

should be used for inspecting screening officers,⁶³⁹ and the underuse of CATSA management for oversight.⁶⁴⁰

All stakeholders should develop and maintain their own systems of oversight and audit. Airport operators, which manage a variety of independent tenants, complained of constraints on their oversight because they lacked the regulatory authority to impose sanctions for non-compliance – powers available only to Transport Canada inspectors.⁶⁴¹ As Transport Canada reviews its regulatory regime, it should consider providing limited enforcement authority to some stakeholders, such as CATSA and airport operators, which supervise other entities.

3.2.2.2.5 Independent Reviews of Aviation Security

In 1985, as a direct result of the bombing of Air India Flight 182, the Government of Canada commissioned the Interdepartmental Committee on Security and Intelligence to undertake a review of airport and airline security in Canada.⁶⁴² Its report, known as the Seaborn Report, was described as a “strategic action plan”⁶⁴³ for Transport Canada, as well as “...a roadmap to take aviation security in Canada from where it was in the aftermath of 1985 to a new and much higher ground.”⁶⁴⁴ The report came to be regarded as a seminal guidance document for aviation security in Canada and around the world.⁶⁴⁵ However, many important recommendations, particularly about air cargo and airport security, were never implemented. This means that civil aviation has remained susceptible to sabotage, despite some security improvements since the release of the report. In 2006, the CATSA Advisory Panel said it was “struck by the similarity”⁶⁴⁶ of many of its own recommendations for addressing deficiencies in aviation security to those that had appeared in the Seaborn Report more than two decades earlier.⁶⁴⁷

The Standing Senate Committee on National Security and Defence published two reviews of aviation security in Canada – one in 2003,⁶⁴⁸ and an update in 2007⁶⁴⁹ – with a focus on security at Canadian airports. The Auditor General of Canada also reviewed various aspects of the civil aviation security regime.⁶⁵⁰

⁶³⁹ Exhibit P-169, p. 88 of 202.

⁶⁴⁰ Exhibit P-173, p. 38.

⁶⁴¹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8161.

⁶⁴² Exhibit P-101 CAF0039, p. 1 of 10.

⁶⁴³ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4504.

⁶⁴⁴ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4505.

⁶⁴⁵ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4504-4505.

⁶⁴⁶ Exhibit P-157, pp. 91-92 of 135.

⁶⁴⁷ Exhibit P-157, pp. 91-92 of 135.

⁶⁴⁸ See, generally, Exhibit P-171.

⁶⁴⁹ See, generally, Exhibit P-172.

⁶⁵⁰ See, generally, Exhibit P-173; see also Exhibit P-411 and *Status Report of the Auditor General of Canada to the House of Commons*, March 2009, Chapter 1: “National Security: Intelligence and Information Sharing”, online: Office of the Auditor General of Canada <http://www.oag-bvg.gc.ca/internet/docs/parl_oag_200903_01_e.pdf> (accessed January 26, 2010) [March 2009 Status Report of the Auditor General of Canada, Chapter 1].

The Commission notes that these reports have assisted in raising public awareness about the inadequacy of aviation security measures in Canada, many of which are applied away from public view. These reports have also led Transport Canada to identify how shortcomings will be addressed. The review by the CATSA Advisory Panel in 2006 was prompted by a requirement in the *CATSA Act* for a review of its provisions and of CATSA's operations, and for a report of the review to be presented to Parliament.⁶⁵¹ The report, *Flight Plan: Managing the Risks in Aviation Security*, led Transport Canada to embark on a systematic review of the recommendations and to report publicly on its progress.⁶⁵²

Although almost 25 years have passed since the Air India bombings, some of the security deficiencies highlighted by the bombing only recently began to be addressed. For example, a comprehensive air cargo security regime is being contemplated to replace the largely vulnerable system that has existed, virtually unchanged, for much of the last two decades.⁶⁵³ Initiatives to extend screening requirements to improve long-known weaknesses in security at FBOs and in the GA sector are being contemplated.⁶⁵⁴ A review of the entire aviation security regulatory regime is in progress.⁶⁵⁵

It is impossible to know the extent to which improvements in aviation security have flowed from these public reports or from the influence of the international community or specific state partners in security. ICAO, for example, conducted a confidential review of Canada's civil aviation security program in 2005, under the Universal Security Audit Program (USAP), to which Transport Canada responded with a confidential Corrective Action Plan.⁶⁵⁶ The initiative to improve air cargo security coincided with a similar drive in the United States.⁶⁵⁷

The Canadian Air Carrier Protective Program (CACPP), which covertly places air marshals on particular flights, was established solely because of a directive issued by the United States immediately following the September 11, 2001, attacks.⁶⁵⁸ The CACPP is a sophisticated program that has received widespread praise and serves as an example of best practices within the international air marshal community.⁶⁵⁹ In contrast, Canada's first "no-fly" list, the Passenger Protect Program, also implemented because of US pressure, has been widely criticized.⁶⁶⁰

651 Exhibit P-175, ss. 33(1), 33(2).

652 See, for example, Exhibit P-101 CAF0871.

653 See, generally, Exhibit P-422; see also Section 3.8.1, which provides a detailed analysis of the deficiencies in air cargo security in Canada.

654 Exhibit P-101 CAF0827, pp. 6-9 of 19; see also Section 3.8.3, which describes the security deficiencies identified at FBOs and in the GA sector.

655 Exhibit P-101 CAF0827, pp. 16-17 of 19.

656 Exhibit P-101 CAF0827, p. 11 of 19.

657 See Section 3.8.1.4, which discusses attempted improvements in the United States and in Canada since 2004.

658 Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8059-8060.

659 See Section 3.1.3.2, which discusses the CACPP in greater detail.

660 See Section 3.5.3.2.1, which discusses the Passenger Protect Program in greater detail.

In May 2009, Transport Canada issued a news release announcing that the 2009 Budget would allocate funds for the development of an airport security plan initiative that was “inspired by the findings and recommendations” of the CATSA Advisory Panel’s 2006 report.⁶⁶¹ The requirement for airport security plans is set out in Annex 17. The Commission heard that, in response to the CATSA Advisory Panel report, Transport Canada established a number of committees in collaboration with CATSA to review the recommendations. Jean Barrette, Director of Security Operations at Transport Canada at the time of the hearings, stated that Transport Canada was working to push the recommendations “... through to fruition and make the necessary changes required to meet the intent and the spirit of the recommendations, as proposed by the Panel.”⁶⁶²

Barrette told the Commission that Transport Canada welcomed the Panel report:

...just like we welcome review from the OAG [Office of the Auditor General], as well as contribution from the [Standing] Senate Committee on [National] Security and Defence.

Transport Canada always sees these reports as an opportunity over and above what we do in approving aviation...security as valuable information and recommendations to always enhance the aviation security program.⁶⁶³

Barrette noted that the recommendations of the Panel did not come as a surprise to the Department and that, in many areas, it had already begun to make improvements.⁶⁶⁴

There have been many influences on aviation security over the past 25 years. The public independent reviews by government bodies and experts have clearly provided an important check on the system, enhancing accountability for security in Canada. Such reports serve as oversight of Transport Canada’s role as regulator. In light of Transport Canada’s interest in moving towards a more performance-based regime and the trend internationally towards self-auditing,⁶⁶⁵ the Commission views further independent, public reviews of aviation security as an ongoing necessity.

As the Seaborn Report concluded in 1985, “...the key to effective security is vigilance, which depends on careful audit and regular testing of the system.”⁶⁶⁶ Despite the ongoing threat of air terrorism, it is well-recognized that when

⁶⁶¹ Transport Canada, “Government of Canada invests in Aviation Security” (Transport Canada News Release, May 5, 2009).

⁶⁶² Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4795.

⁶⁶³ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4795.

⁶⁶⁴ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4795.

⁶⁶⁵ Exhibit P-101 CAF0827, p. 13 of 19.

⁶⁶⁶ Exhibit P-101 CAF0039, p. 10 of 10.

enough time passes without an incident, complacency becomes a danger. Governments have many pressing priorities and their commitment to security can wane as competing interests arise.⁶⁶⁷ Complacency was recognized as a contributing factor in Transport Canada's lack of response to the threat of sabotage before 1985.⁶⁶⁸ The relative lack of aviation terrorism incidents between the 1988 bombing of Pan Am Flight 103 and September 11, 2001, may have also given rise to complacency. This also appears to be the case with air cargo security.

The ongoing threat of terrorist attack and the need to remain alert to the evolving nature of air terrorism do not permit complacency. The Commission therefore recommends a comprehensive and independent review of the civil aviation security regime every five years.

3.2.3 Conclusion

Oversight in civil aviation security includes the establishment of a regime that adequately addresses threats to the system. This requires knowledge of the history of aviation terrorism, as well as constant monitoring of the current threat environment. Any comprehensive regime must begin by meeting the minimum standards outlined by Annex 17, in the spirit with which the provisions were intended. As a prosperous nation, Canada should not only meet, but exceed these standards. Furthermore, to create a system that can best respond to the dynamic nature of aviation terrorism, a Canadian regulatory regime must be proactive, multi-layered, flexible and performance-based, and it must effectively foster an environment of security awareness.

Many entities are involved in civil aviation. A sound aviation security system involves vigilant monitoring of stakeholder compliance and appropriate enforcement. Current penalties for infractions may not be commensurate with the potential consequences of a successful terrorist attack. Canada's inspection and enforcement measures have improved since 1985, but they must improve further to meet the ever growing needs of aviation security.

Stakeholders have an important role in ensuring compliance with security procedures within their own operations. Key to maintaining compliance is clear communication between Transport Canada and stakeholders.

As Transport Canada undertakes a review of its regulatory regime, it must ensure that gaps in security are adequately addressed and that any failure to meet Annex 17 standards is rectified. A periodic independent review of the regime is necessary, along with continued monitoring by the Standing Senate Committee on National Security and Defence and by the Auditor General of Canada.

⁶⁶⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4542.

⁶⁶⁸ Exhibit P-157, p. 54 of 135.

3.3 Risk Management in Aviation Security

Two months before the Air India bombing, the International Air Transport Association (IATA) Director of Security, Rodney Wallis, spoke at the US Federal Aviation Administration's Fourth International Aviation Security Conference. Wallis called for more consistent risk management processes in aviation security. He stated that persistent political unrest throughout the world demanded that at least some attention be paid to political risk analysis, particularly because commercial aviation remained a newsworthy target. He also spoke of the role of risk management in ensuring cost-effective security, given the preceding years of relative economic decline in the international aviation industry. His observations remain relevant today. Risk management that is intelligence-driven and that helps to determine the allocation of limited resources is now viewed as a fundamental part of aviation security. Effective risk management requires systematic and coordinated application across all sectors and between all stakeholders.

Aviation security exists to defend against risks of harm to aviation.⁶⁶⁹ Risk management in aviation security faces several challenges because of the nature of the security risks involved and because resources, both human and financial, are limited.⁶⁷⁰ Unlike risk scenarios involving finance, technology or health, aviation security deals with deliberate attempts to increase risk. Security-related risks involve the element of threat, in which there are attempts to attack and disrupt the system.⁶⁷¹ Threats to aviation are of human design, involve malevolent intent and are calculated to evade detection and prevention.⁶⁷² The primary source of these threats is terrorists, who constantly probe the system for weaknesses. Aviation security has been described as an "intensely dynamic" environment of risk.⁶⁷³

When defensive resources are limited and threats arise from determined and malign extremists, risks can never be completely eliminated.⁶⁷⁴ Although it is

⁶⁶⁹ See Wallis, *Combating Air Terrorism*, pp. xvii-xviii; see also Exhibit P-157, pp. 15-16 of 135 and Exhibit P-149, p. 1.

⁶⁷⁰ Exhibit P-169, pp. 36-37 of 202.

⁶⁷¹ Only a small category of risks involves malevolent intent on the part of human actors. See Testimony of William Leiss, vol. 91, December 7, 2007, p. 11971; Exhibit P-361, Tab 5, pp. 5-6.

⁶⁷² Exhibit P-169, p. 37 of 202.

⁶⁷³ Exhibit P-361, Tab 1, p. 8.

⁶⁷⁴ In addition to the problem of limited resources, additional factors, such as privacy and human rights concerns, as well as the efficient flow of passengers and goods in the aviation industry, also influence the nature and breadth of security measures adopted. As an example, the CATSA Advisory Panel cited the availability of sophisticated new screening technology that produces near-nude images of passengers. While this equipment promises to provide enhanced security, "...concerns over the invasion of privacy and expectations of public resistance have dampened official interest in purchasing such equipment." Nonetheless, this technology has been the subject of pilot studies in Canada and a decision may be made to deploy such equipment for use in pre-board screening. The point is that while the government may have the capacity to take strong security measures, it may in practice face cultural, ethical or political constraints, among others. Such factors are taken into consideration following a risk assessment, as part of the decision-making process when adopting security measures. This is further discussed later in this section. See Exhibit P-169, p. 36 of 202, note 30; see also Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4930.

widely acknowledged that “absolute security is an illusory goal,”⁶⁷⁵ risks must be managed to a level considered acceptable.⁶⁷⁶ As a consequence, risk management in aviation security involves the delicate balancing of an appropriate level of security with finite resources. It requires a principled approach in which a global set of risks is assessed and prioritized to help decide how best to allocate limited resources.⁶⁷⁷ Where responsibility for managing security risks is shared among several entities, as in aviation, full, transparent and clear communication is vital.⁶⁷⁸ In addition, public confidence in aviation security demands that those institutions involved provide adequate disclosure of their methods to manage risk, as well as assurance that resources are optimally used to reduce identified risks.

3.3.1 Risk Management: Introduction

Dr. William Leiss, the Commission’s expert in risk management, defined risk as the “chance of loss or harm” or, more technically, the “probability that some discrete type of adverse effect will occur.”⁶⁷⁹

Risk must not be confused with threat. However, they are related concepts.⁶⁸⁰ Threat is an expression of intention to inflict evil, injury or damage.⁶⁸¹ Threat is an essential component for assessing security-related risks,⁶⁸² and can be identified through intelligence.⁶⁸³ For security-related risks, accurate intelligence is indispensable.⁶⁸⁴

The ultimate goal of risk management is to reduce risk to a predetermined and acceptable level.⁶⁸⁵ In other words, risk management seeks to anticipate and prevent or mitigate serious harms that may be avoidable. This is achieved by applying a reliable method for identifying the highest priority risks to determine appropriate risk control measures. This process assists in allocating risk control budgets across the entire risk spectrum in the most cost-effective manner.⁶⁸⁶ Risk management seeks to inform decision-making by providing full and complete risk estimation (the likelihood that a given threat will cause an incident) and analysis.⁶⁸⁷ In a comprehensive risk management system, no important risks are left unattended.⁶⁸⁸

⁶⁷⁵ Exhibit P-169, p. 36 of 202.

⁶⁷⁶ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11993.

⁶⁷⁷ Exhibit P-169, p. 36 of 202.

⁶⁷⁸ Exhibit P-361, Tab 1, pp. 8-9.

⁶⁷⁹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11978.

⁶⁸⁰ Exhibit P-258, Tab 5, p. 55.

⁶⁸¹ Exhibit P-258, Tab 5, p. 55.

⁶⁸² Exhibit P-361, Tab 5, p. 5.

⁶⁸³ Exhibit P-258, Tab 5, p. 54.

⁶⁸⁴ Exhibit P-101 CAF0873, p. 5.

⁶⁸⁵ Exhibit P-258, Tab 5, p. 55.

⁶⁸⁶ Exhibit P-361, Tab 1, pp. 3-4, 9.

⁶⁸⁷ Exhibit P-361, Tab 5, p. 8.

⁶⁸⁸ Exhibit P-361, Tab 1, p. 9.

Leiss testified that risk management is by no means unique to aviation security, nor is it a novel concept. Financial risk management is a well-established concept⁶⁸⁹ and has served as a foundation for many modern risk management models used in industry.⁶⁹⁰

Leiss testified that the application of formal methods of assessing and managing risk to diverse fields was fairly recent. It was driven primarily by the rising concern over environmental risks in the United States in the 1970s.⁶⁹¹ To provide a more precise method for addressing these risks, the general approach of the financial risk management model was adopted and extended. The science of risk management then developed rapidly. By the 1980s, flow-chart diagrams outlining a standard methodology for managing risks began to appear. Such diagrams consisted of a tightly-ordered sequence of steps, beginning with the identification of a threat or hazard, and ending with a decision about how to manage a risk after all reasonable risk control options had been considered. Health Canada was a pioneer in this area, implementing risk management by 1985. However, it took time for risk management methods to spread to other government departments.⁶⁹²

Leiss stated that the general lack of systematic risk management methods at the time of the Air India bombing did not imply a lack of risk management altogether. Procedures for managing risks were in place, although they did not employ the more ordered, quantitative and probability-oriented approach that has since developed.⁶⁹³

The first official standardized protocols for risk management were developed in the 1990s. These protocols merely formalized methods that were already in use.⁶⁹⁴ Ideally, risks are managed by using a standard methodology that can be applied to any type of risk, ranging from financial to security to public health risks, and within any organization.⁶⁹⁵ Several such standards have been developed around the world.⁶⁹⁶ Canada was one of the first countries to develop its own national standard, issued by the Canadian Standards Association (CSA) in 1997 and entitled *Risk Management: Guideline for Decision-Makers – A National Standard*

689 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11958.

690 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11969.

691 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11968.

692 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11969.

693 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11969.

694 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11962.

695 Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 6.

696 Exhibit P-361, Tab 1, p. 7: Leiss noted the Canadian Standards Association CAN/CSA-Q850-97 (R2007), "Risk Management: Guideline for Decision Makers"; Australian Standard 4360 Risk Management; United Kingdom, HM Treasury, *The Orange Book: Management of Risk – Principles and Concepts* (2004); and the Institute of Risk Management, based in London, to which Canada belongs and which provides materials and training resources upon which Canada relies. Leiss also recommended referring to materials on risk assessment and risk management that are available through the online resource, Wikipedia.

for Canada (CSA Risk Management Guideline).⁶⁹⁷ The International Standards Organization (ISO) is attempting to produce a guide to risk management for use by any entity for any type of risk. A Canadian working group is involved in this effort.⁶⁹⁸ The guide will likely reflect the existing fundamental principles of risk management and will likely be considered the “gold standard” for risk management worldwide.⁶⁹⁹

3.3.2 Risk Management in Aviation Security

The International Civil Aviation Organization (ICAO), through Annex 17 to the *Convention on International Civil Aviation* (“*Chicago Convention*”), requires its member states to implement “to the extent practicable” measures based on security risk assessments carried out by the relevant national authority.⁷⁰⁰ As a signatory, Canada is obliged to comply.⁷⁰¹

The Commission heard frequent references to “risk,” “risk assessment” and, in particular, the need for a “risk-based approach” in aviation security.⁷⁰² Experts and stakeholders, including Transport Canada, emphasized the value of this approach when determining security measures, policies and protocols. Most parties with ongoing responsibilities for aviation security also stated a commitment to this approach.⁷⁰³ However, there was little elaboration of the meaning of these terms.⁷⁰⁴ The CATSA Act Review Advisory Panel (CATSA Advisory Panel), an independent panel of aviation security experts charged with reviewing the *Canadian Air Transport Security Authority Act* (CATSA Act),⁷⁰⁵ warned that such phrases serve to mislead if they are not properly understood.⁷⁰⁶

This vague terminology fails to convey how security measures are selected based on risk. The terms suggest some type of evaluation of risk, but lack detail. This, in turn, fails to instill confidence that risks are being appropriately managed or that a coordinated effort to manage risk exists. The Standing Senate Committee on National Security and Defence (Senate Committee), which has

⁶⁹⁷ This guideline was reaffirmed in 2002 [Canadian Standards Association CAN/CSA-Q850-97 (R2007)]. See Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p.1; see also Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11962-11963.

⁶⁹⁸ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 6.

⁶⁹⁹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11963. As of the time of writing of this report, the ISO risk management guideline has not yet been released.

⁷⁰⁰ Exhibit P-181, p. 2-1, s. 2.2.2.

⁷⁰¹ Annex 17 requirements are considered “minimum standards” that all modern states should be capable of exceeding. See Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4271.

⁷⁰² See Exhibit P-361, Tab 1, pp. 2-3.

⁷⁰³ Exhibit P-361, Tab 1, pp. 1-2.

⁷⁰⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11959.

⁷⁰⁵ The CATSA Act came into effect in March 2002, establishing CATSA as the body responsible for several core aviation security functions. Section 33 of the Act required the Minister of Transport to review the legislation and report the results of the review to Parliament during the Act’s fifth year. On November 23, 2005, the Minister announced the appointment of a three-member Advisory Panel to conduct an independent study and analysis and to prepare a report with recommendations and observations. See Exhibit P-169, pp. 16, 19 of 202.

⁷⁰⁶ Exhibit P-169, p. 35 of 202.

monitored aviation security in Canada since 2001, has expressed concern that assertions of a “risk-based approach” to security policy simply provide an excuse for inaction.⁷⁰⁷

Dr. Kathleen Sweet, a US-based international civil aviation security expert, highlighted the concern over terminology in air cargo security matters. As in Canada,⁷⁰⁸ there is currently very little screening or searching of air cargo in the United States before it is put aboard passenger aircraft,⁷⁰⁹ despite the known risk of sabotage of air cargo.⁷¹⁰ She testified that the US Department of Homeland Security nevertheless professed some comfort with this situation, as long as the stakeholders handling air cargo used adequate “risk assessment” protocols.⁷¹¹ Sweet was critical of this reasoning and cautioned against taking any reassurance from such a statement if stakeholders attribute different meanings to the terminology:

...They use the term “risk assessment,” but how every airline implements that term, how every freight carrier implements that term, how every truck driver that carries the cargo to the airport defines that term, all goes into the mix.⁷¹²

Leiss was also troubled by the apparently loose use of the terms “risk-based approach” and “risk assessment.”⁷¹³ He stated that mere assertions that such an approach or assessment was being followed could not alone provide assurance that robust processes were in place.⁷¹⁴

Despite claims by government agencies and large businesses outside aviation that they employ risk management, there is abundant proof that these same institutions often fail to manage risk effectively.⁷¹⁵ A bleak example was Canada’s failure to appropriately manage the risk of blood-borne infections in blood donated during the 1980s.⁷¹⁶ More recently, the failure of financial institutions to assess and manage the risks associated with certain debt instruments has caused profound and global economic damage.

Risk management is not foolproof. To achieve maximum benefit, its underlying methods must be made as robust as possible. This requires precision in terminology. Leiss testified that risk management derived its strength primarily

707 Exhibit P-169, p. 38 of 202.

708 Exhibit P-169, p. 52 of 202.

709 Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4946.

710 Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4958-4959.

711 See Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4946.

712 Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4946.

713 Exhibit P-361, Tab 1, p. 6.

714 Exhibit P-361, Tab 1, p. 3.

715 Exhibit P-361, Tab 1, pp. 2-3.

716 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11979.

from the use of precise language.⁷¹⁷ Yet risk management has been described as being hampered by semantic confusion.⁷¹⁸

Clear explanation of the terms “risk-based approach” and “risk assessment” is necessary for the public to maintain confidence in aviation security. Where public information is lacking, there can be no assurance of the adequacy of risk management processes.⁷¹⁹ Furthermore, where risk management is a shared responsibility, as in aviation security, miscommunication among stakeholders may occur if they attach different meanings to the same terms.⁷²⁰ Leiss stated that it was entirely possible that all parties shared an understanding of the terms “risk assessment” and “risk-based approach” and that they applied them in the same manner, but that it would be unwise to assume such without further evidence.⁷²¹ He stated that such assumptions could lead to important risks being overlooked.⁷²²

Leiss was critical of the phrase “risk-based approach.” A better characterization, he maintained, was “risk-based decision-making.”⁷²³ A similarly descriptive phrase is “risk management decision-making process,” which has been used to describe the protocol outlined in the CSA Risk Management Guideline.⁷²⁴ Yet Leiss said that even these phrases required further explanation. The underlying process was still not sufficiently clear.⁷²⁵

Those responsible for risk management in aviation security must give assurance that all parties:

- Employ methods that are appropriate according to prevailing professional standards and that are based on current best practices in risk management;
- Set objectives and targets for controlling risk against which performance is measured on a regular basis – ideally, adopting a performance standard of continuous improvement, delivering risk in all relevant areas that is as low as reasonably achievable (ALARA); and
- Achieve acceptable levels of risk control in all of the domains of risk pertinent to civil aviation security.⁷²⁶ [Emphasis in original]

⁷¹⁷ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11959.

⁷¹⁸ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 2. For a comparison of the different meanings attributed to different terms in risk management by various international and national bodies, see Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 3.

⁷¹⁹ Exhibit P-361, Tab 1, p. 3.

⁷²⁰ Exhibit P-361, Tab 1, p. 2.

⁷²¹ Exhibit P-361, Tab 1, p. 2.

⁷²² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11960.

⁷²³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11959.

⁷²⁴ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 4.

⁷²⁵ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11959.

⁷²⁶ Exhibit P-361, Tab 1, pp. 2, 10; see also Testimony of William Leiss, vol. 91, December 7, 2007, p. 12010

In addition, where many parties share responsibility for overall risk management, each should have the same methods, objectives and targets.⁷²⁷ With shared responsibility, the importance of precision in terminology is "...orders of magnitude more serious because you need then further assurance that everybody is on the same page with respect to their methods so that they can compare results."⁷²⁸ The components outlined in the bulleted passage above represent standard aspects of any risk management process that all institutions managing risk should be able to articulate.⁷²⁹ This is particularly important in an area of vital public interest, such as aviation security.⁷³⁰

Describing methods, objectives and targets can be done without compromising the secrecy necessary in security matters.⁷³¹ As will be discussed below, the Canadian Air Transport Security Authority (CATSA) submitted a report to the Commission as a public exhibit, setting out in detail its risk management decision-making process.⁷³² Leiss testified that, by providing such information, institutions with responsibilities in aviation security can instill confidence that risks are being managed appropriately.⁷³³

Leiss identified four "major domains of risk" in aviation security – passengers, non-passengers, cargo and fixed base operations (FBOs).⁷³⁴ The Commission heard ample evidence that at least three – non-passengers, cargo and FBOs – still have significant security gaps.⁷³⁵ The vagueness of the term "risk-based approach" and the possibility that stakeholders will apply it inconsistently leaves the Commission concerned that protection will remain inadequate.

⁷²⁷ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11960-11961.

⁷²⁸ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11961.

⁷²⁹ Exhibit P-361, Tab 1, p. 2.

⁷³⁰ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11959.

⁷³¹ Exhibit P-361, Tab 1, p. 2.

⁷³² Exhibit P-361, Tab 5.

⁷³³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11960.

⁷³⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11960.

⁷³⁵ Exhibit P-169, pp. 52, 55, 68 of 202; see also Exhibit P-172, pp. 17, 29, 58 of 155 and Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5002-5003, 5039, 5041.

Figure 1
Overview of Risk
(Exhibit P-361)

Five Key Activities within a Risk Management Framework ("the overall enterprise"):

- Set goals and focus: identifying context, prioritizing objectives, and setting the scope and focus of the overall exercise. The choices made within this activity are based on a judgment about interests (whose interests count?) and entities (which entities have value?). This is sometimes called "endpoint selection - which risk are we considering?"
- Describe: arriving at an objective understanding of the likelihood and the magnitude of an impact (in qualitative or , better, quantitative terms). As such it is largely a technical or scientific activity.
- Prescribe: evaluating the quality of forecasts provided within the descriptive step, the balancing of positive and negative effects, the decisions on how to mitigate and otherwise manage the risk and the implementation of measures. As such it is evidence and judgement-based activity that requires the consideration of the big picture. It represents the key decision-making step within the risk management framework (which should not imply that decisions of another nature are not taken elsewhere).
- Communicate: communicating among the key actors in the process as well as with the intended beneficiaries and other stakeholders. Communication can be broadly understood as to include public information, consultation, engagement or even partnership. Public designates "the regulated" and other stakeholders.
- Monitor and learn: an activity that describes the monitoring of the effects of decisions and activities that cause changes to the environmental conditions and the emergence of new evidence. Decisions on the need for re-evaluations and the implementation of lessons learned are part of this outcome-oriented activity. These activities are components of performance measurement and results-based management.

The bombing of Air India Flight 182 might well have been prevented if the known risks to aviation security had been better managed. Appropriate risk control measures were available but were not instituted. In the threat environment of 1985, the failure of Air India to institute, and of Transport Canada to require, passenger-baggage reconciliation meant that the risk posed by unaccompanied baggage was not addressed. Passenger-baggage reconciliation was known to be successful in countering the threat of bombs in suitcases.⁷³⁶ Passenger convenience and concerns about delay may have influenced the decision to

⁷³⁶ Exhibit P-101 CAF0163, p. 5; Exhibit P-101 CAF0637, pp. 6, 18.

rely on other security measures for checked baggage.⁷³⁷ However, passenger-baggage reconciliation was the primary defence against a bomb in an unaccompanied bag.

Reliance was placed instead on risk control measures that were known to be ineffective for screening checked baggage for explosives, the precise threat at issue. X-ray machines provided only simple black and white images. Even with skilled operators, the ability of these devices to detect explosives was highly questionable.⁷³⁸ The PD-4 “sniffer” device was employed as a substitute when the X-ray machine broke down. The PD-4 had previously been shown to be ineffective in detecting explosives in checked baggage.⁷³⁹

The decision of the CP Air agent to tag the baggage for interlining to Air India when the passenger had no reservation for the onward journey was critical, and in violation of CP Air’s checked baggage security procedures.⁷⁴⁰ Had CP Air been made aware of the threat environment in which Air India was then operating, it might have prevented unaccompanied baggage from travelling on CP Air flights interlining to Air India.⁷⁴¹ At the very least, CP Air might have exercised greater vigilance in implementing its existing security procedures.

In 1985, the mounting threat that resulted in the destruction of Air India Flight 182 was known by the Government and by Air India. The ability or inability of various security measures to eliminate the threat was also known. Nevertheless, Air India decided to employ methods known to be of questionable use in defeating the threat faced and to waive protective measures where there should have been no discretion.

Many parties now stress the central importance of a “risk-based approach” and of “risk assessment” in aviation security. A more thorough discussion of what these terms mean is necessary. There is a need for clarity, consistency and transparency.

3.3.3 Risk Management Methodology

The Commission sought guidance from Leiss about the key elements of a robust risk management framework for aviation security. He identified the principal components as follows:

- “Anticipate”: Developing the capacity to amass evidence in a timely manner so that proactive, cost-effective measures can be implemented to control risk when the level of risk appears excessive according to some standard;

⁷³⁷ Exhibit P-101 CAF0581, p. 1.

⁷³⁸ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4256.

⁷³⁹ Exhibit P-157, pp. 61-62 of 135.

⁷⁴⁰ Exhibit P-157, pp. 64-65 of 135.

⁷⁴¹ Exhibit P-157, p. 31 of 135.

- “Prevent”: Removing a source of harm in order to eliminate all of the potentially harmful consequences; and
- “Mitigate”: Reducing the anticipated consequences of the harm even when the cause of harm cannot be eliminated.⁷⁴²

The term “risk management” itself is broadly defined in the CSA Risk Management Guideline:

Risk management – the systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and communicating about risk issues.⁷⁴³

In 2004, the External Advisory Committee on Smart Regulation (EACSR), a body established by the federal government, provided a largely similar definition of “risk management.” The EACSR definition summarized the process involved in risk management decision-making:⁷⁴⁴

Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, understanding, assessing, prioritizing, acting on and communicating about potential threats, whether they affect the public’s social, financial or economic well-being, health and safety, or the environment.

Managing the related risk involves allocating limited national resources where they can do the most good for the greatest number of people. It includes the following steps: identification of the issue; assessment of the level and severity of risk; development of the options; decision; implementation of the decision; and evaluation and review of the decision. At each step of the process, communication and consultation activities, legal considerations and ongoing operational activities must also be taken into account in effective risk management strategies.

As indicated in the EACSR definition, risk management decision-making involves a systematic approach – a standard methodology – in which each known harm is addressed to arrive at a decision whether risk control measures are necessary. Although the inputs may be highly diverse⁷⁴⁵ and the analysis may be complex,⁷⁴⁶ the process followed is the same for all known harms. Where

⁷⁴² Exhibit P-361, Tab 1, pp. 3-4.

⁷⁴³ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 2.

⁷⁴⁴ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 2.

⁷⁴⁵ Exhibit P-361, Tab 1, p. 2.

⁷⁴⁶ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11962.

possible, scientific data and statistical analysis are used.⁷⁴⁷ Leiss stated that the “great strength” of risk management was the consistent application of this systematic approach.⁷⁴⁸

Leiss outlined the seven basic steps common to most standardized risk management models:

1. Identifying the threats or hazards;
2. Identifying the exposure to a given threat;
3. Determining the likelihood that a given threat will cause an incident (also known as risk estimation);
4. Identifying the consequences of an incident;
5. Determining the risk and ranking all risks in a matrix;
6. Identifying and implementing risk control options; and
7. Monitoring and review.

All risk management protocols, including the CSA Risk Management Guideline, take a similar approach. Figure 2 contains a schematic model of this approach.⁷⁴⁹

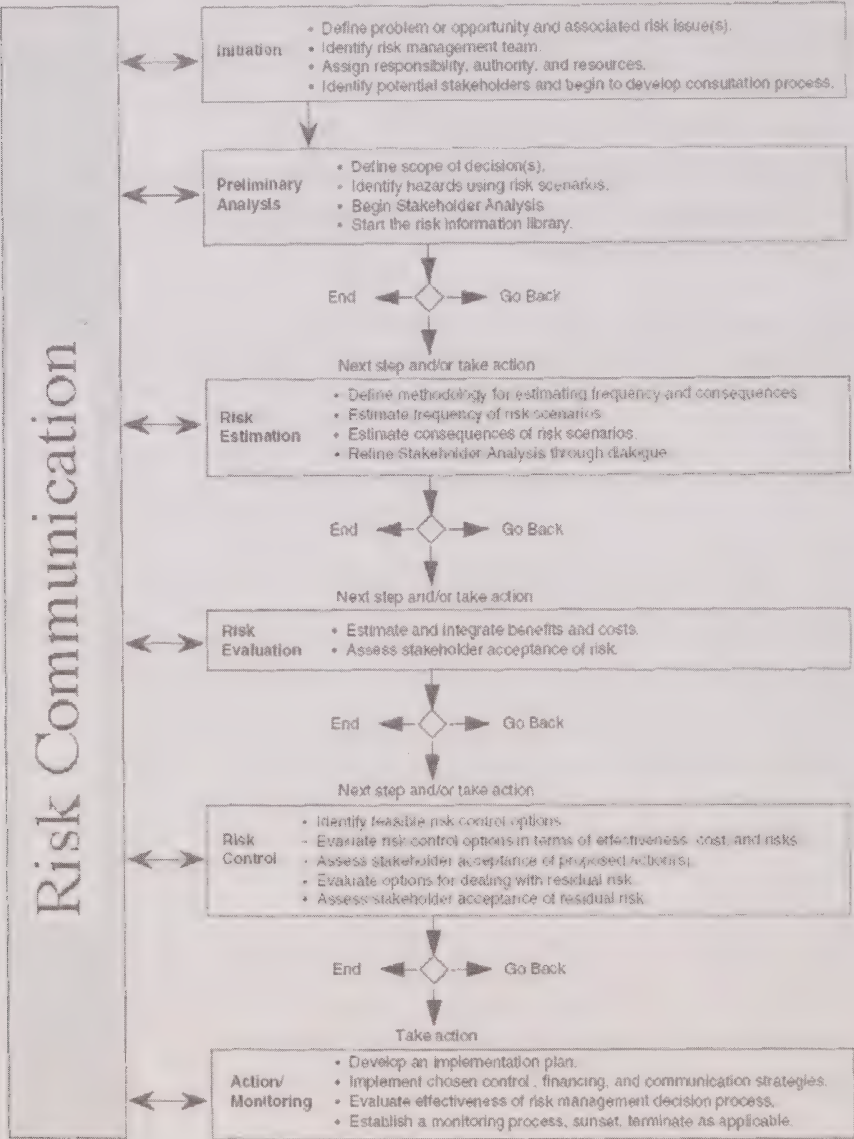
⁷⁴⁷ Exhibit P-361, Tab 1, p. 2.

⁷⁴⁸ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11962.

⁷⁴⁹ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11962-11963.

Figure 2
CSA Risk Management Decision Making-Process
Exhibit P-361

Chart 1: The Risk Management Decision-Making Process According to CSA (1997).
Note: The combination of “preliminary analysis” and “risk estimation” is called “risk assessment”



Source: CSA (1997), p. 7

this includes hazards such as the placement of an explosive device in baggage, cargo or mail, or the commandeering of an aircraft.⁷⁵⁰ The possible level of exposure to each hazard is then examined to arrive at a risk estimation.⁷⁵¹ The two fundamental components of risk estimation are hazard and exposure. The risk estimation represents the likelihood that the hazard and the exposure will intersect to cause an aviation security incident.⁷⁵²

When reasonably good data are available, risks can be expressed in quantitative terms. In the public health sector, for example, the risk in Canada that a unit of donated blood contains HIV is estimated today to be "...1 in 7.8 million donations."⁷⁵³ Quantitative risk estimations also state an uncertainty range, usually expressed as a "95 per cent confidence interval," which provides a range, represented by minimum and maximum values, within which the true risk falls.⁷⁵⁴ No risk estimation is complete without mention of an uncertainty range.⁷⁵⁵

Risk estimations – the assignment of a particular range of risks – must be developed for each individual risk within the range of risks. For example, the four domains of risk outlined by Leiss – passengers, non-passengers, cargo and FBOs – can be further subdivided, and risk estimations calculated for each subdivision.⁷⁵⁶ If sufficient statistical data are not available, a qualitative judgment can be sought, such as an opinion from qualified experts.⁷⁵⁷

The CATSA Advisory Panel cautioned that any risk assessments expressed in quantitative terms must be based on data that "inspire confidence": "...Risk assessments must come with very high standards of accuracy when the margin for error is so small."⁷⁵⁸ The strength of the entire assessment hinges on reliable data. The Panel noted that the degree of certainty and confidence surrounding threats to security presents additional challenges not found with other types of risks. Threats to safety, for example, can be categorized as "malignant threats" since they arise from such measurable matters as design flaws, environmental stress and human error.⁷⁵⁹ Risk assessments must be based on solid data and

⁷⁵⁰ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11963.

⁷⁵¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11964.

⁷⁵² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11964.

⁷⁵³ Exhibit P-361, Tab 1, p. 4.

⁷⁵⁴ For example, maximum and minimum risk estimation values, such as "1 in 3.6 million" and "1 in 20 million," respectively, may be stated to represent the range of risk. This is then interpreted as providing 95 per cent certainty that the true risk is neither higher nor lower than the given range. Applying this confidence interval to the example of the risk of finding HIV in a unit of donated blood, the conclusion can be drawn that the residual risk, after screening and testing, is very low, but not zero. The message that can then be communicated to the public is that the Canadian blood supply has almost certainly never been safer than it is currently, but that the responsible authorities remain vigilant in managing their risk control objectives. See Exhibit P-361, Tab 1, pp. 4-5.

⁷⁵⁵ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11979.

⁷⁵⁶ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11970.

⁷⁵⁷ Exhibit P-361, Tab 1, p. 4.

⁷⁵⁸ Exhibit P-169, p. 37 of 202.

⁷⁵⁹ Exhibit P-169, p. 37 of 202.

on adequate intelligence.⁷⁶⁰ The more information that is available, the more precise one can be in assessing risk.⁷⁶¹

Leiss stated that quantitative measures are preferable, but that an element of judgment comes into play with aviation security risks. Judgment may be required to assess whether the information available amounts to a genuine increase in threat. For example, evaluating the sources of information about a given threat may produce a qualitative “confidence interval.”

Once a risk estimation is established, risk-based decision-making requires understanding the type and magnitude of the consequences of each hazard. Assessing consequences produces an estimate of damage or loss that may result from an identified harm.⁷⁶² This assessment involves identifying immediate and long-term losses, including the number of deaths and injuries, the degree of financial loss, and the possibility that air travel may decline.⁷⁶³

Risk assessment attempts to provide a clear picture of the likelihood (also known as the estimated frequency or estimated probability) and the consequences of exposure to a specific hazard.

The level of risk can be expressed as a product of two factors – likelihood and consequences (Risk = Likelihood x Consequences) – and placed in a “risk matrix,” with likelihood (frequency) and consequences each representing an axis.⁷⁶⁴ Risk is therefore the probability (likelihood) of encountering certain types of consequences.

Figure 3
RISK MATRIX
Exhibit P-361

Appendix D: Risk Matrix

Consequence \ Frequency	Catastrophic	Critical	Marginal	Negligible
High	Class I			
Moderate		Class II		
Low			Class III	
Minimal				
Negligible				Class IV

⁷⁶⁰ Exhibit P-169, p. 38 of 202; see also Testimony of William Leiss, vol. 91, December 7, 2007, p. 11971.
⁷⁶¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11980.
⁷⁶² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11966.
⁷⁶³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11966.
⁷⁶⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11966.

The seriousness of a risk can be ascertained as a function of its level of likelihood, its level of consequences, or both.⁷⁶⁵ One class of risks, “low probability, high consequence,” includes a serious earthquake or a catastrophic failure at a nuclear power plant.⁷⁶⁶

The risk matrix facilitates ranking risks according to the urgency of controlling the risk:

- Class I: Calls for urgent attention and significant risk control measures;
- Class II: Risk control measures are needed;
- Class III: A risk that should be monitored; and
- Class IV: A risk that does not need to be managed.⁷⁶⁷

The risk matrix provides a basis for comparing risks: Class I risks cannot be ignored, while Class IV risks can.⁷⁶⁸ Such a matrix is required where more than one risk must be managed, as in aviation security.⁷⁶⁹

In 1985, for example, the risk of sabotage against Air India would have ranked “high” in a risk matrix, had one been used. Many factors point to such a conclusion. In particular, on June 1, 1985, Air India’s Chief Vigilance and Security Manager in Bombay sent a telex (the “June 1st Telex”) to all Air India offices worldwide, warning that Sikh extremists might try to smuggle explosive devices hidden in baggage onto Air India aircraft. The telex directed Air India stations to ensure the meticulous implementation of counter-sabotage measures for all flights,⁷⁷⁰ and outlined specific baggage screening and airport security measures to be implemented by all operations.⁷⁷¹ In the highly charged and ongoing threat environment facing Air India at the time, the telex’s warning should have featured prominently, and should have been understood as a risk that could not be ignored. When asked about the effect of the warnings that had been received, Wallis responded:

Air India were operating under high risk. They had invoked emergency procedures. So in effect, they were almost putting this on the same level as specific risk.⁷⁷²

⁷⁶⁵ Exhibit P-361, Tab 1, p. 4.

⁷⁶⁶ Exhibit P-361, Tab 1, p. 4.

⁷⁶⁷ Exhibit P-361, Tab 1, p. 12.

⁷⁶⁸ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11970.

⁷⁶⁹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11970.

⁷⁷⁰ Exhibit P-101 CAA0185.

⁷⁷¹ Exhibit P-101 CAA0185.

⁷⁷² Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4415-4416.

The June 1st Telex was shared with some RCMP branches, but not with many other important stakeholders, notably Transport Canada⁷⁷³ and CSIS.⁷⁷⁴

During a document review in October 1987, John Cook, a Special Projects Officer in Transport Canada's Security and Emergency Planning Group, learned of the June 1st Telex.⁷⁷⁵ He wrote that it was "unbelievable" that the telex had not been shared with Transport Canada and that a meeting had not been arranged to discuss "the necessary measures to meet the perceived threat."⁷⁷⁶ Dale Mattson, Transport Canada's Safety and Security Manager at Pearson Airport in 1985, appeared to agree that the telex was a key document respecting the threat of sabotage to Air India. He reported that, had he seen the telex, he would have contacted the Civil Aviation Security Branch for further instructions. Transport Canada had the authority to apply "additional procedures that were needed to address the relevant threat."⁷⁷⁷ Ray Kobzey, a CSIS officer involved in investigating the suspected terrorist activity prior to the bombing of Air India Flight 182, testified that the information in the June 1st Telex would have been "extremely helpful" to his surveillance activities. Specifically, the telex "...may have twigged CSIS to a different interpretation of the "blast" heard in Duncan, British Columbia" because of the reference to time-delayed bombs.⁷⁷⁸ Dr. Reg Whitaker, Chair of the CATSA Advisory Panel, as well as a professor of political science and an intelligence expert, testified that the telex, coupled with the surrounding screening deficiencies on June 23, 1985, would have constituted reasonable grounds for delaying the departure of the Air India flight until security issues could be managed better.⁷⁷⁹

Leiss was told about the June 1st Telex during his testimony and was asked for his opinion about how it would be classified within a risk matrix.⁷⁸⁰ He stated that the telex appeared to provide as specific a warning as is possible in aviation

773 Exhibit P-101 CAA0335, p. 8.

774 Exhibit P-101 CAA0205, p. 34.

775 Exhibit P-367, p. 1.

776 Exhibit P-367.

777 Testimony of Dale Mattson, vol. 29, May 16, 2007, pp. 3215, 3232.

778 Testimony of Ray Kobzey, vol. 33, May 24, 2007, pp. 3810-3811.

779 Testimony of Reg Whitaker, vol. 36, May 30, 2007, p. 4370.

780 In preparing for his testimony, Leiss was provided with key exhibits in the Commission's documentary record pertaining to civil aviation security in the current day and in 1985, as well as to the events surrounding the bombing of Air India Flight 182. These exhibits included the CATSA Advisory Panel's review of civil aviation security in Canada as it relates to the CATSA Act (Exhibit P-169), its review of the civil aviation security issues surrounding the bombing of Air India Flight 182 (Exhibit P-157), Bob Rae's report, *Lessons Learned* (Exhibit P-35), the Auditor General's 2006 Special Examination Report of CATSA (Exhibit P-173), the Seaborn Report (P-101 CAF0039), the Kirpal Commission Report (Exhibit P-164) and the Canadian Aviation Safety Board Report (Exhibit P-167). Subsequent to his testimony, Leiss reviewed the June 1st Telex and associated documents, and was provided with significant background material in relation to the telex and the threat environment at the time. Such material included the Air India disclosure documents pursuant to subpoena (Exhibit P-284) and Air India telexes received by Canadian authorities relating to the period June 1984 to June 1985. Following a thorough review of these documents, Leiss provided the Commission with a sworn affidavit, dated August 20, 2008, reaffirming all of the opinions he expressed during his testimony, without modification. In particular, he confirmed his statements in relation to the June 1st telex. See Exhibit P-433.

security.⁷⁸¹ The telex represented a risk that would have rightly been classified as a high probability risk both in terms of its likelihood⁷⁸² and its consequences.⁷⁸³ Leiss testified that the risk would have been “off the end of the scale in terms of the use of the risk matrix.”⁷⁸⁴ This would have demanded implementing every possible security measure to mitigate the risk, a view that appears to have been shared by both Cook and Mattson.⁷⁸⁵ Yet the information in the telex was not distributed as widely as it should have been, and those who had access to it discussed and acted upon it inadequately.⁷⁸⁶

Leiss was told that the June 1st Telex formed part of a series of warnings that had occurred over a period of time in which no incident had materialized, and that this may have led to some degree of complacency. He stated that, if the reiteration of the threat over a period of time during which no subsequent terrorist incident materialized was in fact interpreted as a diminution of the level of risk, this would have demonstrated “a catastrophic misunderstanding of the nature of risk.”⁷⁸⁷ The lack of a previous incident was immaterial to the level of risk. The persistence of a series of threats should have been a warning in itself.⁷⁸⁸

The CATSA Advisory Panel stated that those responsible for maintaining security are often vulnerable to human error when responding to malevolent threats and that it was common to underestimate the threat before it materialized.⁷⁸⁹ This appears to have been, at least in part, the situation with the June 1st Telex. Maintaining appropriate vigilance and guarding against complacency appear to be as critical in risk assessment and risk management as it is for all aspects of aviation security. Formal risk management protocols were likely not in use to filter and compare risks in 1985, but any risk management process at the time should have identified the telex as having a significant impact on the perceived risk. The history of the June 1st Telex illustrates the role that risk management standards could play in helping to delineate, prioritize and address risks in aviation security systematically.

Once a risk assessment is completed, the results and several other factors are considered in a decision process. These factors may include:

- A risk control options analysis;
- The legal, regulatory and policy framework, both domestic and international;
- Cost-benefit analyses;

⁷⁸¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11982; see also Exhibit P-433.

⁷⁸² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11982; see also Exhibit P-433.

⁷⁸³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11971; see also Exhibit P-433.

⁷⁸⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11982; see also Exhibit P-433.

⁷⁸⁵ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11983; see also Exhibit P-433.

⁷⁸⁶ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 12024-12025; see also Exhibit P-433.

⁷⁸⁷ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11973; see also Exhibit P-433.

⁷⁸⁸ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11974; see also Exhibit P-433.

⁷⁸⁹ Exhibit P-169, p. 37 of 202.

- The public perception of risk, including sensitivity to consequences;⁷⁹⁰
- The sharing of responsibility among various actors; and
- The acceptable level of risk.⁷⁹¹

The relative importance of a factor varies, sometimes considerably, according to the particular risk, time frame and circumstance.⁷⁹²

Risk control objectives, or targets, must be acceptable to the public. Since most risks cannot be managed to the level of zero,⁷⁹³ the objective often becomes to manage the full set of risks to a level that is “as low as reasonably achievable” (ALARA). If the level of risk mitigation for a particular risk does not appear to be acceptable to the public, additional resources may be required.⁷⁹⁴

Security measures should be selected after this multi-step process of evaluating risks and resources has been completed. Implementation requires a commitment of resources as well as communication and coordination with appropriate stakeholders, possibly including the public. Once implemented, ongoing monitoring, evaluation and review are required. Measures may need to change based on new information.⁷⁹⁵ Security measures to which resources have been committed must remain relevant and proportionate to the level of risk.⁷⁹⁶

In emergencies, it may not be possible to analyze potential hazards fully. Intelligence, for example, may show that immediate action is required. The international aviation security community faced this situation in August 2006 with the threat of liquid and gel explosives. Leiss testified that the initial response of banning all liquids and gels from carry-on baggage was appropriate, given the threat and the urgency of the circumstances. Overly-inclusive measures might be needed temporarily, until there was time to fully evaluate whether they were appropriate.⁷⁹⁷ Indeed, Nick Cartwright, Director of the Security Technology Branch, Security and Emergency Preparedness, at Transport Canada, testified that the ban on liquids and gels would not have been sustainable, but was necessary because of the immediate threat at the time.⁷⁹⁸ Upon further evaluation, a decision was made to allow small volumes of liquids and gels in carry-on items, as this continued to mitigate the risk.⁷⁹⁹ Leiss approved of the approach because of the way the threat unfolded.⁸⁰⁰

790 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11967.

791 Exhibit P-361, Tab 1, p. 5.

792 Exhibit P-361, Tab 1, p. 5.

793 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11968.

794 Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11967-11968.

795 Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix E.

796 Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11993, 11997.

797 Testimony of William Leiss, vol. 91, December 7, 2007, pp. 12005-12006.

798 Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5139.

799 Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5140.

800 Testimony of William Leiss, vol. 91, December 7, 2007, p. 12006.

It would also be necessary to evaluate whether the threat should have been identified earlier. In other words, did the “environmental scan” fail to identify the threat beforehand? This evaluation is important because of the ongoing need to examine and improve the procedures for managing risk. Since aviation will face new threats over time, it is essential to determine whether, for example, threat identification protocols remain adequate. Information obtained through such evaluations can be used to improve the protocols.⁸⁰¹

A proactive approach to risk management is essential for strong robust aviation security. The terrorist plot uncovered in 2006 envisaged attacking seven aircraft simultaneously using liquid and gel explosives. The threat was characterized as an “emerging threat”⁸⁰² but it was not new. In 1987, Korean Air Flight 858 exploded over the Andaman Sea after liquid explosives were detonated on board. Two passengers had carried explosives disguised as alcohol from the duty free shop onto the aircraft. Although many governments, including Canada’s,⁸⁰³ claimed to move quickly on the liquids and gels threat in 2006, the Korean Air bombing showed that, long before, the same sabotage technique was used and was largely ignored by governments and the aviation industry. Wallis testified that the response to the liquids and gels threat hardly qualified as “quick.”⁸⁰⁴ Whitaker speculated that the political will to impose such restrictions on passengers had been lacking earlier. However, he suggested, the political will to impose restrictions was found in 2006.⁸⁰⁵

The public perception of risk is merely one of many factors to consider in determining appropriate security measures.⁸⁰⁶ Underestimation of threats is common in aviation security.⁸⁰⁷ The need to be proactive rather than reactive emerged as an important theme during Commission hearings. Terrorists constantly search for new methods of attack,⁸⁰⁸ so risk management must respond to both known and new threats.⁸⁰⁹

In sum, making sound risk management decisions requires adherence to principles that reflect common best practices, including:

1. Risk management methods and protocols, following sequential steps that are widely recognized by professional practitioners in the field;
2. “Robust” procedures for ranking risks and effectively allocating risk control resources across the range of risks;
3. Robust procedures for scanning the environment for novel threats (anticipation of harms), since risk is often a “dynamic environment;”

⁸⁰¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 12006.

⁸⁰² Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5132.

⁸⁰³ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4841.

⁸⁰⁴ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4268.

⁸⁰⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585.

⁸⁰⁶ Exhibit P-361, Tab 1, p. 5.

⁸⁰⁷ Exhibit P-169, p. 37 of 202.

⁸⁰⁸ Exhibit P-169, p. 37 of 202.

⁸⁰⁹ Exhibit P-361, Tab 1, p. 5.

4. Continual updating of risk assessments and risk rankings based on new information, even for threats that are well known;
5. An explicit performance standard against which entities can be held accountable (for example, a “continuous improvement standard” or ALARA); and
6. Regular reporting to stakeholders and the public regarding risk assessment and risk management where serious risks are managed, where this can be done without compromising security.⁸¹⁰

3.3.4 Risk Management Decision-making in Practice

When the Commission asked some stakeholders about their “risk-based approaches” to aviation security, an inconsistent picture emerged. The contrast between the approaches of CATSA and Transport Canada was particularly striking. Leiss reviewed the risk management protocols in each case.

Both CATSA and Transport Canada reported that they used the Integrated Risk Management Framework issued by the Treasury Board Secretariat.⁸¹¹ Leiss criticized the Framework as not being designed for managing public interest risks, but for organizational risks like those that might threaten the integrity of a business entity – for example, financial, human resource and strategic risks.⁸¹² The Framework, he said, was intended only as a general guidance document and could not be considered a rigorous protocol for managing the type of risks involved in aviation security.⁸¹³

Leiss reviewed a summary prepared for the Commission of CATSA’s Risk Management Program.⁸¹⁴ He reported that CATSA had done a very competent job of creating a methodical risk management strategy whose structure was similar to the standard systematic approach. CATSA’s Risk Management Program consisted of two streams, one dealing with organizational risk, as would be expected with the use of the Integrated Risk Management Framework, and another dealing with the management of the types of security risks facing aviation. Under the CATSA Program, a systematic approach was applied to each security risk identified, including:⁸¹⁵

- Listing of discrete risk accompanied by specific background information;
- Expressing probability (likelihood) and impact (consequences) in quantitative terms (percentages) as well as in qualitative terms (low, medium, high, catastrophic);
- Identifying levels of exposure;

⁸¹⁰ Exhibit P-361, Tab 1, pp. 5-6.

⁸¹¹ Exhibit P-361, Tab 3.

⁸¹² Exhibit P-361, Tab 5, p. 5.

⁸¹³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11976; see also Exhibit P-361, Tab 1, p. 7, note 3.

⁸¹⁴ Exhibit P-361, Tab 5.

⁸¹⁵ Exhibit P-361, Tab 5, pp. 6, 12-13.

- Using an appropriate risk matrix, with likelihood and consequences as its axes, to identify the class of risk (low, medium, high, catastrophic);
- Identifying triggering events;
- Determining a prevention plan; and
- Determining a mitigation plan.

Leiss noted, with approval, the explanation of the Program's "impact rating criteria," which consisted of both quantitative and qualitative data. He was satisfied overall with the detail, terminology and methodology provided.⁸¹⁶ He stated that the Risk Management Program presented CATSA's approach to risk management in a way that instilled confidence in the process.⁸¹⁷ Tables 1 and 2 show the criteria that CATSA uses for rating likelihood and impact in qualitative terms.

Table 1
Likelihood Rating Criteria
Exhibit P-361

Table 1: Likelihood Rating Criteria
(Quantitative Measure of LIKELIHOOD over 24 month time horizon)

Level	Likelihood	Description
1	Low	The event is unlikely to occur
2	Medium	The event should occur at sometime
3	High	The event is expected to occur in most circumstances

⁸¹⁶ Leiss advised that he would have preferred an expanded list of criteria related to "damage", fewer criteria related to "reputation loss" and qualitative criteria accompanied by more conventional quantitative terminology, such as "10 to the minus six" (the standard method of expressing "1 in a million"). See Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11987-11989; Exhibit P-361, Tab 5, pp. 6, 7, 12.

⁸¹⁷ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11987-11990.

Table 2
Impact Rating Criteria
Exhibit P-361

Table 2 : Impact Rating Criteria
(Qualitative Measure of IMPACT)

Level	Impact	Damage	Operational Effects	Reputation Loss
1	Low	First Aid Treatment required Asset loss less than \$100K	Schedule delays to minor projects	Setback in building stakeholder trust Some unfavourable media/public attention
2	Medium	Serious injury Asset loss \$100K - \$1M	Disruption of/gaps in essential services for less than 24 hours Schedule delays to major projects	Some loss of stakeholder trust Negative media/public attention
3	High	Death Asset loss \$1M - \$25M	Disruption of/gaps in essential services for less than 7 days Inability to meet operational targets	Significant loss of stakeholder trust Public calls for removal of CATSA executives/ Board members
4	Catastrophic	Numerous deaths Asset loss greater than \$25M	Disruption of/gaps in essential services indefinitely Operational ineffective	Complete loss of stakeholder trust Resignation of CATSA executives/ Board members

It was reassuring to learn that CATSA employed a risk management standard that accorded with common best practices. Transport Canada was unable to provide similar reassurance. Formal risk management standards have been

available in Canada since 1997, but it appears that Transport Canada only recently adopted this approach for aviation security risks. Several reports in recent years have suggested that Transport Canada's risk management strategy in aviation security was deficient. In 2005, a report of the Auditor General expressed disappointment that the Department had not implemented formal risk management protocols.⁸¹⁸ The report criticized the existing risk management system. It found that Transport Canada's approach to assessing security risks in air transport, "to the extent that it has done so," was consistent with the Treasury Board's Framework,⁸¹⁹ but it expressed disappointment that Transport Canada had "not fully implemented formal risk management."⁸²⁰

Specifically, the report found that Transport Canada had not conducted any comprehensive assessment of key risks, nor had it measured the likelihood or potential impact of specific threats.⁸²¹ The report recommended that Transport Canada complete a formal analysis of threats and risks to the entire aviation system which could assist with deploying resources and enforcement efforts.⁸²²

Transport Canada filed the following in response to the Auditor General's report:

Transport Canada recognizes the importance of risk management, which has been an essential foundation of its aviation security program since its inception in the 1970s. More recently, the Department has initiated a comprehensive Transportation Security Strategy, which will examine risk in all modes and activities within each mode. The strategy will include a formal threat-and-risk-analysis instrument that could be used in risk management decision making for regulatory, legislative, and enforcement activities (spring 2006).⁸²³

In 2006, Transport Canada issued a Strategic Security Risk Assessment Methodology and User Guide.⁸²⁴ The CATSA Advisory Panel noted "with approval"

⁸¹⁸ Exhibit P-411, p. 8.

⁸¹⁹ Exhibit P-411, pp. 7-8.

⁸²⁰ Exhibit P-411, p. 8.

⁸²¹ Exhibit P-411, p. 8.

⁸²² Exhibit P-411, p. 9.

⁸²³ Exhibit P-411, p. 9.

⁸²⁴ Transport Canada, *Transport Canada Strategic Security Risk Assessment Methodology and User Guide*, Version 6.0 (March 17, 2006). This is a confidential document that was provided to the Commission following the close of hearings. Transport Canada advised the Commission that this document comprises the risk assessment methodology that is used for civil aviation security. Counsel for the Attorney General of Canada asserted during the hearings that Transport Canada had been "taken by surprise" with the evidence respecting risk assessment and risk management, maintaining that there had been no advance request from Commission counsel regarding Transport Canada's risk management procedures. Commission counsel, on the other hand, indicated that inquiries had been made in advance and that Commission counsel had been referred to the Treasury Board of Canada Secretariat's Integrated Risk Management Framework. See Transcripts, vol. 91, December 7, 2007, pp. 12042-12043.

in its 2006 report that Transport Canada had conducted at least one exercise in which aviation threats were measured quantitatively, ranked and assessed according to risk. However, the Panel noted the lack of further exercises.⁸²⁵ Leiss testified that these reports provided little confidence that Transport Canada regularly applied appropriate risk management processes. The use of the approach in one instance did not provide sufficient reassurance.⁸²⁶

The Commission asked Transport Canada to confirm that the Strategic Security Risk Assessment Methodology and User Guide represented the current expression of Transport Canada's approach to risk management and risk assessment. In response, the Attorney General of Canada requested an in-person briefing for Commission counsel with Transport Canada representatives, to ensure that the intricacies of risk assessment and risk management would not be overlooked in a simple response to these questions. Leiss attended this briefing in his capacity as an expert.

During the briefing, Transport Canada officials confirmed that there were no further documents to describe its approach to managing security risks. They maintained that the Methodology and User Guide was developed only after considerable consultation with experts and that it was consistent with industry standards, including the CSA Risk Management Guideline.⁸²⁷ The Commission was told that a risk matrix was used, but Transport Canada officials were unable to articulate a consistent means for assessing and managing risk. In addition, although it appears that risk management was beginning to be discussed at the Advisory Group on Aviation Security (AGAS), a multi-stakeholder forum for addressing security issues in Canada, Transport Canada did not appear to be fully informed about the risk management processes used by various stakeholders.⁸²⁸ For instance, Transport Canada informed the Commission that it was not necessarily aware of the risk management methodology employed at the local level by air carriers.⁸²⁹

Transport Canada advised the Commission that it was "... making significant progress ... to establish an aviation security performance measurement framework."⁸³⁰ On the issue of public accountability, the Department stated that public confidence relied on the overall aviation security program, and that such confidence was an underlying objective of risk assessment. However, Leiss stated that it was not the purpose of a risk assessment to set a level of adequate performance in the management of a risk.⁸³¹ A risk assessment described the likelihood of an adverse outcome and, if it occurred, the possible consequences. This gave the risk manager an idea of the severity of a risk. The risk manager

825 Exhibit P-169, p. 37 of 202, note 33.

826 Testimony of William Leiss, vol. 91, December 7, 2007, p. 11990.

827 Exhibit P-101 CAF0873, p. 3.

828 Exhibit P-101 CAF0873, p. 4.

829 Exhibit P-101 CAF0873, p. 4.

830 Exhibit P-101 CAF0873, p. 5.

831 Exhibit P-101 CAF0873, p. 5.

would then have to apply some standard of risk control – for example, ALARA (“as low as reasonably achievable”) – if the existing level of risk appeared too great.

The evidence provided to the Commission suggests that Transport Canada is not using an appropriate standard protocol for risk management decision-making in aviation security, based on a common set of protocols, using current best practices and operating under a performance standard of continuous improvement to arrive at levels of risk that are as low as reasonably achievable. Perhaps a comprehensive, systematic approach is in place, but Transport Canada did not give the Commission sufficient reassurance of this.

Transport Canada is the national authority responsible for the development, maintenance and oversight of civil aviation security in Canada. It has the lead role as policy-maker and regulator.⁸³² The Commission expected that Transport Canada would have provided direction in establishing and requiring risk management procedures, after appropriate consultation.

Systematic approaches to risk assessment and risk management were introduced to government in 1985, and a national standard was developed by 1997. By 2007, risk assessment and management protocols were well established in Canada. Transport Canada should have been able to articulate methodically the approach that it uses for risk management, for all types or categories of risk.

The Commission also noted the varying approaches to risk management among others in aviation security. In particular, IATA outlined an approach that defined risk as comprising three factors – “threat,” “vulnerability” and “criticality.” It described its approach as consisting of five basic steps:⁸³³

- Accurately identifying the risk;
- Assessing the consequences of risk exploitation and likelihood of exploitation;
- Finding and identifying measures to protect against, control or eliminate a certain risk;
- Assessing the measures for their effectiveness and consequences; and
- Implementing measures to ensure that each risk is appropriately managed.

IATA’s goal is to “... reduce the probability that a particular risk will be exploited.”⁸³⁴ The approach involves using a “threat response matrix” to determine whether a threshold level has been reached to support using certain security measures and undertaking consequence assessments, also known as “assessing criticality.”

⁸³² Exhibit P-169, p. 30 of 202.

⁸³³ Exhibit P-258, Tab 5, p. 56.

⁸³⁴ Exhibit P-258, Tab 5, p. 56.

Many terms used by IATA differ from those used in other discussions of risk management, and the IATA approach does not follow the standard approach precisely. However, it appears to offer a systematic, methodical means of addressing all risks.

Yves Duguay, Director of Security for Air Canada at the time of the Commission hearings, described an intelligence-driven approach that reviews “vulnerabilities,” “probabilities” and “impact on industry.”⁸³⁵ Again, there was some sense of a systematic approach, although further inquiry would be necessary to assess Air Canada’s risk assessment methodology properly.

Stakeholders sometimes appear to describe similar aspects of risk management using different terms. It is important for each party to be able to understand the risk management processes being described by the other parties so that they can intelligently compare and discuss approaches.

A 2005 report of the US Government Accountability Office recommended adopting a risk-based management approach to aviation security in the US. Like the IATA approach, that of the US included setting strategic goals and objectives, assessing risk (threat, vulnerability and criticality), evaluating alternatives, selecting initiatives, and implementing and monitoring those initiatives.⁸³⁶

3.3.5 Matching Limited Resources with Risk Control Objectives

Resources for managing risks are limited. An institution’s “risk budget” must be allocated across the full set of risks in a defensible way. One approach is to use cost-effectiveness, or maximum benefit per unit of expenditure, with the overall caveat that no important risk be neglected. Public expectations and good risk management practices demand that specified risks be controlled to a level that is regarded by the public as “acceptable” and that no gaps remain in the system.⁸³⁷

Leiss testified that every major enterprise has a risk management plan for all the risks they face. A global budget, usually annual, provides for “enterprise risk management.” Each type of risk, including financial, occupational and health, is allocated a portion of the budget. Choices must be made in allocating the limited resources to maintain risks at an acceptable level.⁸³⁸

Governments manage entire sets of risks under one budget. The risks posed to aviation security are only one type of risk that Transport Canada manages.⁸³⁹ Within aviation security itself, risks can be divided and subdivided into a number of categories. Leiss testified that an allocation must be made to aviation

⁸³⁵ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5238.

⁸³⁶ Exhibit P-417, p. 3.

⁸³⁷ Exhibit P-361, Tab 1, p. 9.

⁸³⁸ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11991-11992.

⁸³⁹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11992.

security as a whole and that sub-allocations are required for categories such as passengers, non-passengers, cargo and FBOs. He said that, ideally, allocations should be proportionate to the risk presented by each category.⁸⁴⁰ The risk matrix could assist in deciding allocations.⁸⁴¹

Leiss stated that answering two main questions can help determine whether risks have been appropriately managed in the face of limited resources:

1. Are resources sufficient to manage risks to an acceptable level? If not, have additional resources been sought?
2. Have resources been allocated wisely?⁸⁴²

The position of Leiss can be summarized as follows: Managing several independent risk factors simultaneously within the same envelope (such as passengers, non-passengers, cargo and FBOs) requires achieving a predetermined level of acceptable risk for each. It may be possible to rebalance resources to achieve this. If rebalancing resources is not sufficient, additional resources must be found.⁸⁴³

The case of air cargo security is instructive. The Commission heard much evidence that significant gaps remain in aviation security. The most troubling relates to air cargo.⁸⁴⁴ The CATSA Advisory Panel referred to air cargo as "...a major security gap, perhaps the single most significant gap that has been brought to our attention. Air cargo is largely unscreened at present, and this represents a serious vulnerability in the system."⁸⁴⁵ Both Wallis and Sweet also identified air cargo as among the weakest links in aviation security,⁸⁴⁶ one recognized for nearly 30 years but still not addressed adequately.⁸⁴⁷ Sweet testified that security resources have been disproportionately weighted towards screening passengers and their baggage, and away from air cargo. She stated that, paradoxically, this worked to the detriment of passenger security:

...[W]e have focused so much on passengers and passenger baggage that we have failed to recognize that there is a huge part of that aircraft that is loaded up with pallets of cargo that is moved round with passengers on board, and how and where and when that cargo is screened is a huge gap....⁸⁴⁸

⁸⁴⁰ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11993.

⁸⁴¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11999.

⁸⁴² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11993.

⁸⁴³ Exhibit P-361, Tab 1, p. 9.

⁸⁴⁴ Exhibit P-169, p. 52 of 202; see also Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4329.

⁸⁴⁵ Exhibit P-169, p. 52 of 202.

⁸⁴⁶ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003; see also Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4958-4959.

⁸⁴⁷ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

⁸⁴⁸ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4942.

Transport Canada is now attempting to address the air cargo security gap.⁸⁴⁹ It informed the Commission that a risk assessment was conducted before the Air Cargo Security Initiative (ACS Initiative) was developed, but provided no details that would show rigour in its approach.

Simply because air cargo has not yet been implicated in a major security incident does not alter the level of risk. As with the June 1st Telex in 1985, the absence of an incident should not play a role in decisions about risk management where there is evidence of an ongoing threat.⁸⁵⁰ Wallis testified, however, that it is tempting to cut costs when an incident fails to materialize:

If you go a few years without an incident, then you will even reach the stage where politicians will want to try to divert money to some other source because you do not need it; nothing is happening. That's what you have to guard against....⁸⁵¹

There has been some criticism that the "risk-based approach" to aviation security may be used to hide inaction, particularly if serious security shortcomings remain.⁸⁵² The CATSA Advisory Panel agreed that risk management should not be conducted superficially or used as an "ex-post facto rationalization for inaction," but it did not entirely support the premise about how a risk-based approach might hide inaction. The Panel provided the following reasons:⁸⁵³

- Government resources are not unlimited;
- Security policy is not the sole priority of government or the Canadian public; and
- Threats to security are not of equal magnitude or urgency.

The Panel advised that limited resources must be deployed after careful risk assessments.⁸⁵⁴ The Commission agrees that decisions based on best practices and standard protocols offer the greatest promise for addressing risks and deploying resources in aviation security.

3.3.6 Shared Responsibility and Accountability

Civil aviation security in Canada is a shared responsibility. Transport Canada is the regulatory authority with ultimate responsibility, but several government bodies share operational responsibilities. These include CATSA, the RCMP and local police. Other stakeholders, such as air carriers and airport operators, are

⁸⁴⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5183.

⁸⁵⁰ Testimony of William Leiss, vol. 91, December 7, 2007, p. 12003.

⁸⁵¹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4771-4772.

⁸⁵² Members of the Standing Senate Committee on National Security and Defence have expressed doubt that a risk-based approach is an adequate solution for serious security shortcomings. See Exhibit P-169, p. 38 of 202; see also Exhibit P-171.

⁸⁵³ Exhibit P-169, p. 38 of 202.

⁸⁵⁴ Exhibit P-169, p. 38 of 202.

also involved. CSIS provides Transport Canada with intelligence relating to security.⁸⁵⁵ However, shared responsibility brings with it the danger of missing important security risks and measures to address them.⁸⁵⁶ Seamless coordination is required to avoid gaps.⁸⁵⁷

Agencies all need to follow the same methods and protocols for risk management decision-making. Each agency should be able to explain clearly to all partners the structure and protocols of its “risk-based approach” and should provide regular updates. Discrepancies in the protocols must be identified and resolved. Once stakeholders share an understanding about the methods followed, each stakeholder can safely rely on the information or analysis provided by the others. Stakeholders can achieve seamless coordination only if they all meet both regularly and on an as-needed basis.⁸⁵⁸

Transport Canada created the Advisory Group on Aviation Security (AGAS) in 2005 to provide a secure forum for government and industry stakeholders to exchange views about aviation security policies and initiatives.⁸⁵⁹ The mandate of AGAS is to provide information to stakeholders about current and emerging security priorities and to receive “high-level strategic advice” from them.⁸⁶⁰ Five technical subcommittees of AGAS deal with particular security issues – aerodromes, security screening, air carriers, air cargo security and Security Management Systems (SeMS).⁸⁶¹ The CATSA Advisory Panel described AGAS as playing an important consultative role at the national level. Representatives from the Canadian Airports Council (CAC) and the Airline Pilots Association, International (ALPA), both of which participate in AGAS, praised its effectiveness.⁸⁶² Fred Jones, Vice President of Operations and Legal Affairs at the CAC, described the main benefit of AGAS:

...[Y]ou get a better end regulatory result; you have a better regulatory policy when you can understand the viewpoints of all stakeholders in the aviation community through a face-to-face exchange....⁸⁶³

The existence of AGAS is encouraging, but the Commission saw little evidence of coordination of risk management among stakeholders. The evidence points to the contrary conclusion. Yet, AGAS appears to be an ideal forum for dealing with risk management. Risk management principles are a fundamental element of decisions in aviation security, and the Commission sees merit in moving quickly to ensure clear and coordinated efforts within AGAS.

⁸⁵⁵ Exhibit P-169, pp. 30-33 of 202.

⁸⁵⁶ Exhibit P-361, Tab 1, p. 8.

⁸⁵⁷ Exhibit P-361, Tab 1, pp. 8-9.

⁸⁵⁸ Exhibit P-361, Tab 1, pp. 8-9.

⁸⁵⁹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8117; see also Exhibit P-169, p. 49 of 202.

⁸⁶⁰ Exhibit P-169, p. 49 of 202.

⁸⁶¹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8117.

⁸⁶² Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8117; see also Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7999.

⁸⁶³ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8117.

Failing to share responsibility effectively in aviation security can lead to consequences such as those leading to the bombing of Air India Flight 182. The mishandling of the June 1st Telex provides a prime example of a breakdown in risk communication among the entities responsible for security. The main stakeholders were Transport Canada, the air carriers, the RCMP and CSIS.⁸⁶⁴ It appears that both Air India and certain branches of the RCMP reviewed the telex,⁸⁶⁵ but it also appears that there were no follow-up discussions, nor was the telex shared with other stakeholders, notably CSIS and Transport Canada.⁸⁶⁶ Leiss was highly critical of this failure:

...[G]iven the specificity of that threat collectively, in terms of Air India's corporate responsibility, it seems appalling that you would not follow up, you would not find out what would be done with that information. You would not insist on having a meeting, a further dialogue of trying to see whether you could actually work out a common plan and not say, "Well, do whatever you want with this," but say "what can Air India and the Canadian Government and police forces do together to lower the risk that's involved. Or, what other options do we have to control the risk involved?"⁸⁶⁷

The bombing of Air India Flight 182 was preventable. It represented a true failure of shared responsibility in aviation security. As Bob Rae observed in his report, *Lessons Learned*:

Despite the precautions and protections that were supposed to be in place, almost everything that could have gone wrong did go wrong. The bags should never have been checked without an accompanying passenger in Vancouver. Canadian Pacific Flights 060 (Vancouver to Toronto) and 003 (Vancouver to Narita) should not have taken off without a reconciliation that would have shown no accompanying passenger for these bags aboard either flight. When the bag arrived in Toronto from Canadian Pacific Flight 060 it should not have been transferred to the Air India plane without being checked and a bag reconciliation taken.

However, the suitcase with the bomb did get through 2 airports, both in Vancouver and Toronto. The mid-air explosion off the west coast of Ireland in the early morning of June 23, 1985, was the consequence.⁸⁶⁸

⁸⁶⁴ Exhibit P-157, pp. 22-24 of 135.

⁸⁶⁵ Exhibit P-157, p. 30 of 135.

⁸⁶⁶ Testimony of J.B. MacDonald, vol. 27, May 14, 2007, p. 2865; Exhibit P-101 CAA0335, p. 8.

⁸⁶⁷ Testimony of William Leiss, vol. 91, December 7, 2007, p. 12025.

⁸⁶⁸ Exhibit P-35, p. 11.

The bombing of Air India Flight 182 was only possible because of aviation security failures by several stakeholders. Each stakeholder failed to manage its risks properly:

- CP Air failed to follow its own baggage security procedures;
- Air India was inexcusably careless in deploying checked baggage screening devices and procedures that it ought to have known were inadequate for the purpose, and it failed to prevent unauthorized bags from being loaded onto the aircraft;
- Transport Canada, on behalf of the Government of Canada, failed in its role as regulator by denying Air India the security support it required and by permitting Air India to rely on inadequate security procedures and plans; and
- Air India, Transport Canada and the RCMP each failed to assess threat and intelligence information appropriately and to communicate this information adequately to relevant stakeholders.

Today, air cargo appears poised to become the next example of a failure to share responsibility appropriately in risk management. This is despite air cargo security being the focus of one of the technical subcommittees of AGAS. Those responsible for air cargo security should coordinate their efforts. They should learn about and develop an understanding of the efforts of others, and use complementary methods and protocols to address security issues. Stakeholders should hold regular discussions to stay abreast of the efforts of others.

Leiss testified that enhanced public accountability is also required to reassure the public that there is adequate coordination among stakeholders and that risks are being properly addressed.⁸⁶⁹ Public accountability requires assurance from stakeholders that they are all using a standard protocol – ideally, the same standard protocol – for risk management decisions.⁸⁷⁰ Leiss also maintained that the ranking of aviation security risks within the risk matrix should be disclosed and justified in order to maintain public confidence that the allocation of resources is rational. He said it would not be a breach of security to disclose the methods and language used.⁸⁷¹

However, Transport Canada did not give the Commission any information about which, if any, methods for assessing and managing risk are currently used in Canada. Other stakeholders also appeared to have difficulty in obtaining this information from Transport Canada. The Commission heard from the Office of the Privacy Commissioner about its discussions with Transport Canada about the Passenger Protect Program, a passenger screening initiative aimed at preventing persons who are considered potentially harmful to aviation from boarding a flight (also involving what is colloquially called a “no-fly” list). Lindsay Scotton,

⁸⁶⁹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11961.

⁸⁷⁰ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11997.

⁸⁷¹ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11997.

the Privacy Impact Assessment Review Manager in the Privacy Commissioner's office, was asked whether she knew of any risk-based assessment conducted by Transport Canada to justify the program:

The answer to that is no. That was one of our specific recommendations in our response to the Privacy Impact Assessment, which was, "Please show us the assessments, the studies, quantitative or qualitative, that would ... justify the substantial intrusion into the privacy rights of Canadians." We haven't received such a study, so the answer to that is no.⁸⁷²

Transport Canada did not provide any information to the Commission that would allow it to conclude that the Department had completed a risk assessment for the Passenger Protect Program.

A 2002 report of the United Kingdom's Strategy Unit on Risk and Uncertainty, *Improving Government's Capability to Handle Risk and Uncertainty*,⁸⁷³ outlined five principles for managing risks in the public interest. These might inform the development of a more robust risk management decision-making process in Canada:

Openness and Transparency

Government will make available its assessments of risks that affect the public, how it has reached its decisions, and how it will handle the risk. It will also do so where the development of new policies poses a potential risk to the public. When information has to be kept private, or where the approach departs from existing practice, it will explain why. Where facts are uncertain or unknown, government will seek to make clear what the gaps in its knowledge are and, where relevant, what is being done to address them. It will be open about where it has made mistakes, and what it is doing to rectify them.

Involvement

Government will actively involve significant stakeholders, including members of the public, throughout the risk identification, assessment and management process. This will support timely and targeted action. Two-way communication will be used in all stages of policy development, risk assessment and risk management. Where there are differences in interpretation it will aim to clarify these through open discussion, and it will seek to balance conflicting views in a way that best serves the wider public interest. It will explain how views obtained through consultation have been reflected in its decisions.

⁸⁷² Testimony of Lindsay Scotton, vol. 72, November 6, 2007, p. 9017.

⁸⁷³ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 20.

Proportionality and Consistency

Government will seek to apply a consistent approach to its assessment of risks and opportunities and to its evaluation of the costs and benefits of options for handling them, and will ensure that these are clearly articulated. It will apply the precautionary principle where there is good reason to believe that irreversible harm may occur and where it is impossible to assess the risk with confidence, and will plan to revisit decisions as knowledge changes.

Evidence

Government will aim to ensure that all relevant evidence has been considered and, where possible, quantified before it takes decisions on risk. It will seek impartial and informed advice that can be independently verified wherever possible, and seek to build a shared understanding of the risks and options for action. It will consider evidence from a range of perspectives, including the public as well as experts.

Responsibility

Government, where possible, will ensure that those who impose risks on others also bear responsibility for controlling those risks and for any consequences of inadequate control. It will aim to give individuals a choice in how to manage risks that affect them, where it is feasible and in their interest to do so and where this does not expose others to disproportionate risk or cost.⁸⁷⁴

3.3.7 Culture of Security

One of the great failures of the aviation security regime in 1985 was the general lack of a security culture.⁸⁷⁵ The current national standard for risk management in Australia and New Zealand specifically advocates a holistic approach that brings “risk management thinking” into the culture of an organization, its business practices and everyday activities:

To be most effective, risk management should become part of an organization’s culture. It should be embedded into the organization’s philosophy, practices and business processes rather than be viewed or practiced as a separate activity. When this is achieved, everyone in the organization becomes involved in the management of risk.⁸⁷⁶

⁸⁷⁴ In 2001, the British Prime Minister announced the creation of a Strategy Unit on Risk and Uncertainty. In 2002, the Strategy Unit published a comprehensive report, *Risk: Improving government’s capability to handle risk and uncertainty*. This report introduced a number of ideas that go beyond the information contained in the CSA Risk Management Guideline, including the listing of the five *Principles of Managing Risks to the Public*, as outlined above. See Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, pp. 20, 23.

⁸⁷⁵ Exhibit P-157, p. 72 of 135.

⁸⁷⁶ Exhibit P-361, Tab 5, Additional Documents for Tab 1, Appendix E and Appendix F, Appendix F, p. 12.

The Commission heard evidence of a move towards a culture of greater security awareness through the Security Management Systems (SeMS). The SeMS approach requires all individuals and departments within the aviation environment, regardless of their particular duties or mandates, to help maintain overall security.⁸⁷⁷ The CATSA Advisory Panel described SeMS as a “risk-based approach” and identified it as a necessary basis for any aviation security regime.⁸⁷⁸

For SeMS to be effective, an organization must embrace security as part of its overall business so that “...security becomes a culture that percolates throughout the entire organization.”⁸⁷⁹ In addition to requiring a security policy, a process of goal-setting about security objectives, training of personnel and internal and external reviews of the system, the SeMS approach requires:

- A process for identifying security risks and evaluating and managing the associated responses; and
- A process for the internal reporting and analysis of threats, incidents and breaches and for taking corrective actions to prevent similar incidents.⁸⁸⁰

SeMS is an evolving concept.⁸⁸¹ There appears to be confusion among stakeholders about its meaning and application.⁸⁸² Transport Canada made no mention of SeMS during a briefing of Commission counsel on risk management.⁸⁸³

A culture of security awareness requires awareness of risk management practices. The Commission encourages the further development of SeMS, a process that should involve consultation with all stakeholders, along with coordinated efforts in risk management decision-making. This too requires clarity, precision in terminology and transparency amongst stakeholders, so that all participants have the same understanding of what is required under this system. The Commission is skeptical about poorly understood and abstract concepts being held out as solutions. It remains to be seen whether SeMS will improve aviation security.

⁸⁷⁷ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8111.

⁸⁷⁸ Exhibit P-169, p. 37 of 202.

⁸⁷⁹ Exhibit P-169, p. 93 of 202.

⁸⁸⁰ Exhibit P-169, p. 94 of 202.

⁸⁸¹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8114.

⁸⁸² Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8000.

⁸⁸³ Exhibit P-101 CAF0873.

3.3.8 Conclusion

The terms “risk-based approach” and “risk assessment” were used liberally during Commission hearings, with little explanation of and little apparent regard for their precise meanings. Although this created an impression of rigorous management of security, the evidence often suggested otherwise. Even when pressed, Transport Canada officials could not articulate a consistent means by which the Department manages risk in aviation security. Furthermore, although responsibility for security is shared among many stakeholders, there was little evidence of coordination or a system-wide risk management strategy.

Because there is no systematic approach to risk management, significant risks may go unnoticed. Serious gaps already exist in aviation security. It is essential that a risk management decision-making process be established and implemented quickly.

The evidence before the Commission leads to the conclusion the aviation security system should have the following characteristics:

1. A common set of protocols for carrying out risk management;
2. Risk management protocols and methods based on current best practices in the field;
3. A performance standard of continual improvement, delivering levels of risk in all relevant areas that are as low as reasonably achievable; and
4. Acceptable levels of risk control in all of the domains of risk pertinent to aviation security.

3.4 Use of Intelligence in Aviation Security

As discussed elsewhere in this report,⁸⁸⁴ the collection and analysis of critical intelligence about threats to civil aviation in the years leading up to the bombing of Air India Flight 182 lacked coordination, and any sharing of that intelligence was unstructured and inconsistent.⁸⁸⁵ A key lesson of the bombing was that aviation security is diminished by unwarranted constraints on the flow of intelligence and other threat information. Due to a general climate of excessive secrecy, information was frequently not shared with concerned parties, such as air carriers and Transport Canada. This was exemplified by the institutional preoccupation with the “need to know” principle. Even when threat information was being disseminated, the lack of secure communications channels slowed the arrival of the information where it was needed, limiting the ability of airports and air carriers to respond to threats.

⁸⁸⁴ See for example, Volume Two: Part 1, Pre-Bombing, Section 4.4, Failures in Sharing of Information.

⁸⁸⁵ See Testimony of Reg Whitaker, vol. 36, May 30, 2007, pp. 4310-4312.

These intelligence failures resulted in air carriers that interlined passengers and their baggage to Air India – for example, CP Air – operating as if normal security conditions prevailed, even though Air India faced a serious risk of terrorist attack. CP Air took no extraordinary security precautions in June 1985, and took no steps to remove the interlined checked bag belonging to “M. Singh” when he failed to board CP Air Flight 060. CP Air breached its own security program in two ways: by agreeing to interline the bag even though Singh did not have a reservation on Air India Flight 182, and by failing to offload the bag from Flight 060 once CP Air became aware that he did not show up for the flight. There is good reason to believe the airline would have been much more vigilant if it had known of the threat facing Air India.

The *Canadian Air Transport Security Authority Act* (CATSA) Review Advisory Panel concluded that any effective aviation security program must be “...intelligence-led, based upon up-to-date threat assessments and resilient enough to adapt to new threats as they emerge.”⁸⁸⁶ Rodney Wallis, former Director of Security at the International Air Transport Association (IATA), has long contended that intelligence has a crucial role to play in confronting terrorism.⁸⁸⁷ Similarly, Yves Duguay, Senior Director of Air Canada Security and the Chairman of the IATA Security Committee, testified that the best security system was intelligence-driven.⁸⁸⁸ The aviation security program in place in 1985 was deficient because it focused on the waning threat of hijacking and on called-in “specific threats” as the exclusive triggers for emergency action. Peter St. John, a retired professor of international relations with expertise in air terrorism, testified that the lack of better intelligence about the threat before the Air India bombing could itself be seen as a failure by Canada’s intelligence community to co-operate and to establish appropriate systems for discerning such threats.⁸⁸⁹

After the Air India bombing, Transport Canada established the Security and Emergency Preparedness Directorate⁸⁹⁰ to deal with transportation security. The Directorate is responsible for policy development, intelligence, the transportation security clearance program, and security training guidelines for its security inspectorate and for industry. It is concerned with all modes of transportation overseen by Transport Canada, not merely aviation.

The intelligence failures leading up to the bombing led to changes in how intelligence relating to terrorism and aviation security was collected, analyzed and disseminated. Still, it was only after the attacks of September 11, 2001, that Canada’s intelligence community began to shift its operational focus from a culture of secrecy marked by the “need to know” mentality to a focus that contemplated a “need to share.” The “need to share” concept was discussed in the Hon. Bob Rae’s report, *Lessons to be Learned*, in relation to the notorious reluctance of US agencies to share information before the September 11th

⁸⁸⁶ Exhibit P-169, p. 26 of 202.

⁸⁸⁷ See, for example, Exhibit P-148, p. 9.

⁸⁸⁸ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5238.

⁸⁸⁹ Testimony of Peter St. John, vol. 38, June 1, 2007, pp. 4573-4576.

⁸⁹⁰ Exhibit P-157, p. 83 of 135.

attacks, as well as in relation to the institutional firewalls between the RCMP and CSIS.⁸⁹¹

The CATSA Advisory Panel stated that, as aviation security continues to tighten, terrorists could be expected to shift tactics and seek out and target as-yet-unnoticed weaknesses or “the unknown unknown.”⁸⁹² This increased the need for intelligence gathering and threat assessments. The Panel added that, since 2001, the Government of Canada placed a much greater emphasis on the integration of intelligence gathering and analysis, as well as on the broader and timely dissemination of this information.⁸⁹³ Even so, many obstacles that impeded the proper flow of information in 1985 persist today, particularly tensions between the producers and consumers of aviation security intelligence over its sharing.

3.4.1 Integrated Threat Assessment Centre

Among the aviation security and intelligence reforms undertaken since 2001 was the creation of the Integrated Threat Assessment Centre (ITAC). ITAC was established in October 2004.⁸⁹⁴ It produces comprehensive threat assessments focused exclusively on terrorism.⁸⁹⁵ There was no such integrated capacity in 1985.⁸⁹⁶ ITAC was created in recognition of the fact that “...the current scope of threat assessment requirements exceeds the capacity of any one organization.”⁸⁹⁷ Many of Canada’s allies had already developed integrated intelligence organizations, and ITAC would enhance Canada’s ability to participate as an equal in the international intelligence community and protect Canadians.

ITAC operates out of CSIS. It has access to CSIS information and is staffed by personnel seconded from a broad cross-section of government organizations, including Transport Canada, CSIS, the RCMP, the Department of National Defence, the Canada Border Services Agency, and the Communications Security Establishment.⁸⁹⁸ ITAC distributes its threat assessments to its core intelligence community partners, including Transport Canada, which is represented at ITAC by the Security and Emergency Preparedness Directorate.⁸⁹⁹ Transport Canada then provides this information to related stakeholders, including CATSA, as it considers appropriate. The CATSA Advisory Panel stated that one of ITAC’s most valuable contributions was its ability to make intelligence and other classified or restricted threat information available to recipients in a form appropriate to the recipient’s level of security clearance.⁹⁰⁰

⁸⁹¹ Exhibit P-35, p. 23.

⁸⁹² Exhibit P-169, p. 38 of 202.

⁸⁹³ Exhibit P-169, p. 42 of 202.

⁸⁹⁴ Testimony of John Schmidt, vol. 53, September 27, 2008, p. 6643.

⁸⁹⁵ Exhibit P-157, p. 107 of 135.

⁸⁹⁶ Exhibit P-157, p. 107 of 135.

⁸⁹⁷ Testimony of John Schmidt, vol. 53, September 27, 2008, p. 6644.

⁸⁹⁸ Exhibit P-223, Tab 4, p. 4.

⁸⁹⁹ Exhibit P-169, p. 42 of 202.

⁹⁰⁰ Exhibit P-157, p. 107 of 135.

Dr. Reg Whitaker, chair of the CATSA Advisory Panel, testified that, since 1985, there had been a move to integrate and coordinate the various actors involved in the intelligence process.⁹⁰¹ This required a shift away from the “information silos” and turf wars of the past, characterized by intelligence failures and preventable tragedies. According to the Panel, ITAC’s place within the intelligence community was an example of both horizontal and vertical integration. Horizontal integration occurred, for example, when ITAC drew on a wide range of sources and served the broader intelligence community in producing security threat assessments.⁹⁰² Vertical integration involved channels for providing intelligence to its many consumers. For example, ITAC and CSIS threat assessments were passed to Transport Canada and then to CATSA.

3.4.2 Information Sharing: Canadian Air Transport Security Authority

CATSA told the CATSA Advisory Panel that CATSA depended on timely and accurate intelligence to manage its daily operations, to plan long-term strategic policies and to facilitate more effective screening by front line officers.⁹⁰³ For this reason, the Standing Senate Committee on National Security and Defence, in its 2003 report, *The Myth of Security at Canada’s Airports*, recommended that CATSA develop its own intelligence capabilities.⁹⁰⁴ The Committee repeated this recommendation in the 2007 *Canadian Security Guide Book*, and also recommended that CATSA receive all available intelligence related to aviation security.⁹⁰⁵

CATSA officials argued that CATSA did not have sufficient access to the intelligence essential to its operations. In addition, they wanted a seat at the ITAC table.⁹⁰⁶ The CATSA Advisory Panel concluded, however, that Transport Canada remained the most appropriate recipient of strategic intelligence information about terrorism, which it could then disseminate to CATSA.⁹⁰⁷

Jim Marriott, Director of the Aviation Security Regulatory Review for Transport Canada, testified that the Department “actively shared” with CATSA the security-related information it needed.⁹⁰⁸ The CATSA Advisory Panel also found that CATSA was receiving appropriate intelligence.⁹⁰⁹ Whitaker suggested that CATSA’s concern that it was not receiving sufficient intelligence might be fueled in part by the prestige and mystique attributed to intelligence stamped “Top Secret,” and by the envy felt by those who thought that information was being withheld from them.⁹¹⁰

⁹⁰¹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4570-4571.

⁹⁰² Exhibit P-169, pp. 42-43 of 202.

⁹⁰³ Exhibit P-169, p. 44 of 202.

⁹⁰⁴ Exhibit P-171, p. 129 of 256.

⁹⁰⁵ Exhibit P-172, p. 76 of 155.

⁹⁰⁶ Exhibit P-169, p. 46 of 202.

⁹⁰⁷ Exhibit P-169, p. 46 of 202.

⁹⁰⁸ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4803.

⁹⁰⁹ Exhibit P-169, pp. 44-46 of 202.

⁹¹⁰ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4581-4582.

The Standing Senate Committee on National Security and Defence made a valid point in 2003, however, when it stated that "...CATSA, as an arm's length security agency, will have a hard time staying one step ahead of people with bad intentions if it does not have an intelligence component.... [S]urely security training is *based* on intelligence."⁹¹¹ As discussed below, there is considerable value in providing front line personnel with usable, actionable⁹¹² intelligence through regular briefings or security updates. This is already done to some extent and should be encouraged further. The sharing of intelligence keeps front line personnel aware of current threats, boosts their motivation and morale and instills a genuine sense of mission. The value of sharing intelligence with those whose work requires vigilance but is often perceived as monotonous and lacking prestige cannot be overstated.

The CATSA Advisory Panel described three types of intelligence that CATSA wanted: actionable, issue-specific or tactical, and strategic.⁹¹³ Whitaker testified that CATSA did receive actionable intelligence relevant to its screening mandate.⁹¹⁴ The Panel stated that it was "...[c]learly ... in the interests of the travelling public and national security for actionable intelligence to be provided to those who can act upon it." However, the Panel did not think it necessary for CATSA to receive intelligence about individuals or groups that might be a threat to aviation, since CATSA screening officers did not check identity documents and were concerned solely with searching for dangerous objects.⁹¹⁵

Intelligence that was "issue-specific" or "tactical" might involve information about new types of improvised explosive devices or new ways of concealing weapons.⁹¹⁶ One example of tactical intelligence was that about the threat, publicized in the summer of 2006, of terrorist attacks against aircraft using liquid-based explosives. This led to a ban on liquids and gels in carry-on baggage.⁹¹⁷ Here, the necessary intelligence was rapidly communicated to Canadian authorities. CATSA was immediately advised and it quickly implemented new security measures. This successful coordination and CATSA's response were described as "an intelligence victory"⁹¹⁸ and a "textbook example" of how the system ought to work.⁹¹⁹

The third type of intelligence – strategic – was described by CATSA as "...the type of intelligence needed to enhance its understanding of all aspects of the terrorist threat, including motivating factors, ideological underpinnings, main objectives, financing, modus operandi and operational support base." The CATSA Advisory Panel noted CATSA's desire to "...be at the table at ITAC along

⁹¹¹ Exhibit P-171, p. 123 of 256 [Emphasis added].

⁹¹² The CATSA Advisory Panel described "actionable intelligence" as "threat information that requires immediate response": Exhibit P-169, p. 44 of 202.

⁹¹³ Exhibit P-169, p. 44 of 202.

⁹¹⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4577-4578.

⁹¹⁵ Exhibit P-169, p. 45 of 202.

⁹¹⁶ Exhibit P-169, p. 45 of 202.

⁹¹⁷ Exhibit P-169, p. 45 of 202.

⁹¹⁸ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 7945-7946.

⁹¹⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4584-4585.

with Transport Canada and the other [intelligence producers].” However, it saw no clear advantage to ITAC or to the strategic intelligence community from CATSA’s participation, since CATSA was primarily an intelligence consumer and only a limited producer of intelligence. The Panel concluded that “...Transport Canada remains the appropriate channel from ITAC as the integrated analyst to CATSA as consumer.”⁹²⁰

Wallis testified that CATSA should not go beyond its core screening specialization and “re-invent the wheel” by developing an intelligence function. He stated, however, that it was essential for Transport Canada to ensure that CATSA received all information relevant to its operations.⁹²¹ The CATSA Advisory Panel also urged closer co-operation between Transport Canada and CATSA in sharing intelligence.⁹²²

According to the Final Submissions of the Attorney General of Canada, Transport Canada and CATSA were working to implement the CATSA Advisory Panel’s recommendations and to ensure that CATSA “...receives all the intelligence required and that both organizations have a continuous learning environment in 2008.”⁹²³

3.4.3 Information Sharing: Aviation Security Partners

The sharing of intelligence by government agencies with others involved in aviation security, such as air carriers, airports and front line workers, must be addressed. As the Panel noted, the threat environment requires that “...front-line actors be provided with real-time, actionable intelligence capable of warning against and pre-empting attacks.”⁹²⁴

The Canadian Airports Council (CAC) has 46 airport authority members, collectively operating about 180 airports in Canada. This membership accounts for 95 per cent of the passenger volume and almost all cargo and international operations in the country.⁹²⁵

Aviation stakeholders need to be informed about threats to airports and aircraft. They must, as the CATSA Advisory Panel recommended, be kept abreast of other changes to the threat environment to be able to respond adequately to new threats, rather than being forced to react at the last minute.⁹²⁶ Regular security briefings for all stakeholders are warranted, including briefings for front line workers that will boost morale and promote a sense of mission.

⁹²⁰ Exhibit P-169, p. 45 of 202.

⁹²¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5013-5014, 5031-5032.

⁹²² Exhibit P-169, p. 46 of 202.

⁹²³ Final Submissions of the Attorney General of Canada, Vol. II, para. 330.

⁹²⁴ Exhibit P-169, p. 43 of 202.

⁹²⁵ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8105.

⁹²⁶ Exhibit P-169, p. 47 of 202.

Fred Jones, Vice President of Operations and Legal Affairs for the CAC, testified that many CAC members were concerned about a lack of timely access to intelligence.⁹²⁷ One particular concern was the inability to transmit pertinent information securely. Transport Canada responded by creating a secure system, the Secure Remote Access Security Database (SRAS), to distribute and access security information measures. It also had the potential to transmit intelligence. Jones testified, however, that even when security information was sent to airports, it was not always timely or complete and it might not reach the right people in time for them to take appropriate action.⁹²⁸ The CATSA Advisory Panel also reported that several airlines complained that they were not receiving information and threat assessments on a timely basis.⁹²⁹

Jim Bertram, Director of Public Safety for the Greater Toronto Airports Authority (GTAA), also testified that timely delivery of intelligence was an ongoing problem. He also called for confusion over the types of information certain groups wanted to be addressed:

.... Canada is one of the world leaders in its ability to gather and analyze intelligence. We do that very well through the RCMP, through CSIS, Transport Canada. And I think the first question that we ask is simply: what is intelligence?

There are a large number of groups, even within our own airport, that would like almost on a daily basis the dumping of raw data, as opposed to analyzed data or intelligence. So they haven't yet articulated what they mean when they say they want something. They want more intelligence. They're not saying what it is. So we first of all need to identify what that is and then allow the people that collect it and analyze it or cause them to share that information with people that do need it.⁹³⁰

Airport authorities and other stakeholders that want more intelligence risk becoming inundated. The important issue is not the quantity of information that a stakeholder receives, but the relevance of the information to the stakeholder's activities.

Bertram saw a serious danger in reacting to intelligence that had not been analyzed and assessed. Jones agreed, testifying that receiving quality intelligence was essential. A way was needed to distill the vast amounts of security information and intelligence into a refined, actionable form, while ensuring its prompt delivery to stakeholders.⁹³¹

⁹²⁷ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8119-8120.

⁹²⁸ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8119-8120.

⁹²⁹ Exhibit P-169, p. 41 of 202.

⁹³⁰ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8120-8123.

⁹³¹ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8172-8173.

Bertram testified about the organizational problems in providing timely, relevant intelligence to airport authorities:

.... [T]he airport authority is a not-for-profit organization. It is not a law enforcement agency. And law enforcement agencies that are responsible for collecting and analyzing and creating intelligence don't have the authority in a lot of cases to give me particularly, as the Director of Public Safety, information that affects our airport. By law they can share it with other enforcement agencies but they can't share it with me. So that is a glitch in the system and does cause some timeliness concerns for us.⁹³²

Bertram added that government agencies would decide what intelligence information was important to an airport. He stated that more complete threat information about aviation security should instead be passed on to the airports to use as they saw fit. He had seen some improvements, but the concerns of airports about timeliness and quantity and access to intelligence were only slowly being addressed.⁹³³

IATA stated that "...much more work needs to be done by regulators to share intelligence information with airlines. There is a distinct 'need to share' not only during regular operations but in times of emergency operation as well. All [too] often we find regulators stubbornly fixated on the 'need to know' paradigm."⁹³⁴

Georgina Graham, the Global Head of Security and Facilitation for IATA, testified about IATA's concerns about the need to share:

And too often governments say that in terms of security information, "We will tell you what we think you need to know," but the airline needs to be able to do its own risk assessments, its own threat and risk assessments and to work out where its own vulnerabilities are, and you really need robust intelligence to be able to do that effectively.

... [P]articularly with the events of August 2006 in the foiled U.K. terror plot, what we saw there was the government having good intelligence data and using that data wisely, and letting the industry know what was happening and prevented something from occurring. And that is what we need to see, the ability to share data between regulators and our airlines, and in the industry, to ensure the best use of that data to prevent these acts of unlawful interference from occurring in the first place.⁹³⁵

⁹³² Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8120-8121.

⁹³³ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8120-8121.

⁹³⁴ Exhibit P-258, Tab 1, p. 12.

⁹³⁵ Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8240.

Such lines of communication must, of necessity, be established between states and their airlines rather than through IATA. The airlines will be the direct recipients of the intelligence. IATA must continue to promote security management systems and information sharing within the aviation industry.

Steps have been taken to ensure that the local police at airports have the security clearances required to receive intelligence about threats. Jean Barrette, Director of Security Operations at Transport Canada, testified that the policing community was a very important source of local intelligence⁹³⁶ and that information frequently passed from the local police to Transport Canada and CSIS, and vice versa. Duguay testified that, at Toronto's Pearson Airport, Air Canada was taking part in an intelligence exchange with Peel Police, the RCMP and CATSA, through daily advisories.⁹³⁷ Air Canada was also working with government departments to establish national security committees among the roughly 62 agencies involved in security, as well as to establish local security committees for each airport.

Dr. Kathleen Sweet, a US-based aviation security expert, testified that giving screeners intelligence instilled motivation and a greater sense of mission and purpose. She discussed a pilot project at Dulles International Airport where screening personnel received regular intelligence briefings. She described it as an "absolutely great" program that gave them "a bit of intelligence" and made them feel important.⁹³⁸ The screeners regularly received low-level but pertinent intelligence about potential threats and upcoming events that merited particular vigilance. The screeners were also trained about suspicious "flags," such as a passenger wearing a bulky, heavy coat on a hot day.

Pierre Cyr, Vice President of Strategic and Public Affairs at CATSA, testified that it would be difficult to implement a similar program in which CSIS briefed the screeners at all 89 designated airports each day. However, CATSA screening officers regularly received security information from in-house sources.⁹³⁹ This was done through daily briefings by screening point leaders and area managers, as well as through CATSA Screening Operations Bulletins and Transport Canada Security Notices. Screening officers were expected to read these documents.

Captain Jean Labbé, Security Coordinator of the National Security Committee of the Air Line Pilots Association, International (ALPA), testified that pilots did not have adequate access to intelligence about threats to aviation.⁹⁴⁰ He stated that, although the industry worked on a "need to know basis," pilots *had* a need to know; they should be made aware of threats to their flights and should also be privy to broader intelligence concerning threats to aviation as a whole. Labbé stated that pilots were an important part of security, and that making them

⁹³⁶ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4803-4804.

⁹³⁷ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5280-5281.

⁹³⁸ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4968-4969.

⁹³⁹ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4809-4810.

⁹⁴⁰ Testimony of Jean Labbé, vol. 64, October 23, 2007, p. 8001.

aware of possible concerns, along with threats and security risks, could only improve security.

Captain Craig Hall, Director of the National Security Committee of ALPA, shared Labbé's views about the importance for pilots of access to intelligence.⁹⁴¹ Hall stated that a small, select group of airline pilot representatives did occasionally receive high-level briefings in response to requests for further information on a specific topic.⁹⁴² He did not say that pilots required raw intelligence or that they should be considered for top secret security clearance, but rather that they should receive information appropriate to their duties.⁹⁴³

Hall stated that intelligence flowed in two directions. Pilots required information about the conditions under which they operated aircraft, to help them make appropriate and informed decisions. As well, if properly briefed, pilots could provide extensive observations about matters that should be reported, but that were not necessarily being reported. He described pilots and crew as an untapped intelligence resource. Some 100,000 aircraft pilots were directly engaged in the aviation system each day and saw changes in conditions all over the world. An even larger number of flight attendants interacted with passengers.⁹⁴⁴

3.4.4 Conclusion

Canadian aviation security in 1985 lacked coordination and communications. Organizational conflicts limited the effective use of intelligence. Canada has made significant progress since then in collecting and analyzing intelligence and in distributing it promptly to aviation stakeholders. The creation of ITAC, its vertical and horizontal integration between intelligence producers and consumers, and its ability to distribute information in a form appropriate to recipients' security clearance levels, clearly represent significant improvements.

Still, substantial disagreement remains about access to intelligence between high-level producers of intelligence and front-line consumers. The "need to know" continues to be accepted by those who produce the information and resisted by those at the front lines. The clear consensus of the many security experts and stakeholders heard by the Commission was that more work was needed to ensure that a reflexive "need to know" approach does not dominate the "need to share" approach, and to ensure that the need to share is reflected in practice. Much of the work of aviation security takes place not only within intelligence agencies, but also on the front lines.

The Commission stresses the critical importance of ensuring that those concerned with airport and aircraft security receive focused, adequate and actionable intelligence in a timely fashion.

⁹⁴¹ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 8002-8003.

⁹⁴² Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8035.

⁹⁴³ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 8002-8003.

⁹⁴⁴ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 8002-8003.

An uncritical acceptance that the existing flow of information about aviation security is adequate must be avoided. As in the past, the organizations that produce and disseminate intelligence, threat assessments and other security information might conclude that the current level of sharing is adequate. Complaints from those on the front lines, such as CATSA, that too little intelligence is reaching them, and suggestions that CATSA might need to develop intelligence-producing capacities, help to substantiate the argument that intelligence is not being provided in a timely manner to those on the front lines. Behind the thinking of those on the front line is a fear of a disaster occurring because an intelligence producer unwisely concluded that an intelligence consumer had no need for a particular item of intelligence. In short, all participants in the intelligence and aviation security communities must constantly assess whether the information necessary to protect civil aviation is reaching, in time, the people who need it.

3.5 Passenger and Baggage Screening

Passenger and baggage screening was designated as a central aspect of the Commission's mandate in aviation security, to be examined within the context of lessons learned from the bombing of Air India Flight 182.⁹⁴⁵ Indeed, the screening of passengers and their carry-on and checked baggage is a core element in the defence of civil aviation.⁹⁴⁶ Before 1985, aviation security measures focused on screening passengers and carry-on baggage,⁹⁴⁷ since the primary aim at the time was to prevent aircraft hijackings.⁹⁴⁸ Despite knowledge by government of a generalized risk of sabotage,⁹⁴⁹ little emphasis was placed on screening the checked baggage to be loaded into the hold of an aircraft, except in certain cases of heightened threat.⁹⁵⁰ This changed with the bombing of Air India Flight 182. In response to this and later sabotage incidents worldwide – in particular, the bombing of Pan Am Flight 103 and the terrorist attacks of September 11, 2001 – layers of screening measures for passengers, carry-on and hold baggage were built up to address this threat, each complementing the other.

A comprehensive system for passenger and baggage screening now exists in Canada. A government agency, the Canadian Air Transport Security Authority (CATSA), has been established to deliver screening services for passengers and baggage, removing this key responsibility from air carriers. Passengers and baggage are screened using much more sophisticated technology than was available in 1985,⁹⁵¹ with enhanced capabilities for detecting prohibited items, including explosive devices. Passenger-baggage reconciliation and

⁹⁴⁵ Para. b(vii) of the Commission's Terms of Reference called for findings and recommendations to address "whether further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, **particularly those relating to the screening of passengers and their baggage**" [Emphasis added].

⁹⁴⁶ Exhibit P-169, p. 16 of 202.

⁹⁴⁷ Exhibit P-157, p. 17 of 135.

⁹⁴⁸ Exhibit P-157, p. 75 of 135.

⁹⁴⁹ Exhibit P-263, Tab 5, p. 15

⁹⁵⁰ Exhibit P-263.

⁹⁵¹ Exhibit p-157, p. 103 of 135.

a multi-tiered process for full hold bag screening (HBS) together provide the best defence available against bombs in checked baggage.⁹⁵² Passengers are also subjected to layers of screening that involve metal detectors and that may also involve hand searches and inspection by explosive trace detection units at secondary or random screening. Besides being required to produce a boarding pass, passengers must show valid photo identification at the boarding gate.⁹⁵³

Passenger screening is becoming increasingly intrusive. As more invasive screening technology is considered for routine use, concerns about individual privacy rights have been raised, challenging the relative unassailability of the traditional “no search, no fly” principle. A profound shift also appears to be taking place in the conceptualization of passenger screening itself, with a focus not only on the detection of prohibited objects, but also on the identification of individuals who pose a danger to aviation. Canada has recently instituted its own “no-fly list” under the Passenger Protect Program, and is evaluating behavioural analysis techniques for screening. Such measures have the potential to violate rights, including those protected by the *Charter*.⁹⁵⁴ Indeed, the constitutionality of the Passenger Protect Program is currently being challenged in the Federal Court of Canada by the first (and, to the Commission’s knowledge, the only) individual to be denied boarding privileges under its auspices.⁹⁵⁵

Although an impressive, multi-layered approach to passenger and baggage screening has been developed since 1985,⁹⁵⁶ other vulnerabilities in civil aviation remain, exposing passengers and aircraft to the risk of sabotage. Aviation is secure only if all vulnerabilities are appropriately addressed. These vulnerabilities are discussed in other parts of this volume.⁹⁵⁷

3.5.1 Post-1985 Developments

3.5.1.1 Hold Bag Screening

Within months of the bombing of Air India Flight 182, Transport Canada made passenger-baggage reconciliation mandatory for international flights, later extending the measure to domestic flights.⁹⁵⁸ Passenger-baggage reconciliation

⁹⁵² In Canada, *Air Regulation 812*, dated December 17, 1974, directed air carriers to examine checked baggage on aircraft in the event of a specific threat: see Exhibit P-157, p. 56 of 135. Internationally, the 1983 ICAO *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference* suggested that passenger-baggage reconciliation be conducted where a flight was “...believed to be the subject of a specific threat” or where air carriers were operating at airports that were considered to be in “high risk areas.”: Exhibit P-157, p. 57 of 135. Air India’s Security Programme in Canada provided for increased checked baggage security as part of its Emergency Procedures: see Exhibit P-157, pp. 27-28 of 135. In 1984, KLM and CP Air together implemented a passenger-baggage reconciliation measure in response to a bomb threat: see Exhibit P-101 CAF0637, pp. 18-19.

⁹⁵³ Exhibit P-157, p. 103 of 135.

⁹⁵⁴ Wallis, *Lockerbie*, p. 154.

⁹⁵⁵ See Exhibit P-426.

⁹⁵⁶ Exhibit P-157, p. 86 of 135.

⁹⁵⁷ See Section 3.8.

⁹⁵⁸ Exhibit P-35, p. 20.

involves correlating passengers with their baggage to verify that passengers with checked baggage have actually boarded the aircraft.⁹⁵⁹ It addresses the danger presented when ill-intentioned passengers voluntarily separate themselves from their baggage – that of a bomb in unaccompanied baggage.⁹⁶⁰ It deals with the principle that passengers and their baggage must be treated as a single entity, a principle arising directly from the events that led to the loss of Air India Flight 182.⁹⁶¹ Not only was Canada the first country to require passenger-baggage reconciliation on international flights, but it played a lead role in persuading the international community to adopt this measure as a standard to be incorporated into Annex 17 to the *Convention on International Civil Aviation* (“*Chicago Convention*”).⁹⁶² In the immediate aftermath of the Air India bombing, methods of automating passenger-baggage reconciliation procedures were established to enable the measure to be implemented in larger centres with high passenger volumes.⁹⁶³ In 1988, the then-President of the International Civil Aviation Organization (ICAO) Council described passenger-baggage reconciliation as “the cornerstone of security against the baggage bomber.”⁹⁶⁴ Today, it is still considered a key defence against sabotage.⁹⁶⁵

However, passenger-baggage reconciliation alone is not sufficient because it does not account for the “unwitting accomplice” who unknowingly introduces a bomb on board an aircraft.⁹⁶⁶ In 1986, a Palestinian terrorist placed a bomb in the hand baggage of his Irish fiancée, without her knowledge. The bomb was destined for an Israeli jumbo jet, but the bomb’s discovery before she boarded the flight prevented the destruction of the plane.⁹⁶⁷ In addition, passenger-baggage reconciliation cannot counter a suicide bomber who knowingly boards an aircraft with an explosive device in checked baggage,⁹⁶⁸ a threat which has become increasingly prevalent.⁹⁶⁹

Effective technology for screening explosive devices is also required.⁹⁷⁰ Unlike the summer of 1985, vastly-improved explosives-detecting technology is now available for screening hold baggage.⁹⁷¹ After 1985, research and development projects at Transport Canada focused on eliminating some technological deficiencies that had figured in the Air India bombing. Projects included the development of X-ray pattern recognition and enhancement of capabilities for detecting trace explosives.⁹⁷² At the time of the bombing, Transport Canada

959 Exhibit P-157, p. 58 of 135.

960 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4476.

961 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477.

962 Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4722.

963 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4478; see also Exhibit P-157, p. 86 of 135.

964 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4237.

965 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4507.

966 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4257.

967 Testimony of Peter St. John, vol. 35, May 29, 2007, p. 4250.

968 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4257.

969 Testimony of Peter St. John, vol. 35, May 29, 2007, p. 4251.

970 Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4257.

971 Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4415; see also Section 3.6, which describes the technology currently being used and considered for civil aviation security.

972 Exhibit P-157, p. 86 of 135.

was already testing explosive vapour detection (EVD) units for screening hold baggage, but had not yet deployed them at airports.⁹⁷³ Following the loss of Flight 182, these units were rapidly commercialized and installed in airports across the country. In the years that followed, the technology became increasingly sophisticated and reliable.⁹⁷⁴

Even then, the technology was “nowhere near as refined”⁹⁷⁵ as it is today. Following the bombing of Pan Am Flight 103, which was destroyed by plastic explosives concealed in unaccompanied interlined hold baggage, significant research and development efforts were devoted to methods for screening hold baggage for explosives and for introducing these technologies into the airport environment.⁹⁷⁶ In 1995, the first series of EVD units were replaced with a new generation of portable equipment that could detect plastic explosives.⁹⁷⁷ A few years later, images produced by X-ray equipment, including that used for screening carry-on baggage, improved from black and white images (which were known in 1985 as unreliable and even merely “cosmetic”) to “dual-energy” colour X-ray imaging capable of detecting explosives and organic material.⁹⁷⁸

Following the Pan Am bombing, renewed emphasis was also placed on requiring full hold bag screening (HBS). Both full HBS and passenger-baggage reconciliation are required to address adequately the threat of bombs in checked baggage:

Airports that have in place passenger and baggage reconciliation systems...and have introduced baggage screening in a multilayered security program have already moved to minimize the possibility of an improvised explosive device being carried in a suitcase.⁹⁷⁹

Since January 1, 2006, in accordance with Annex 17 of the *Chicago Convention*, all hold baggage has been screened at all of Canada’s designated airports. Up to five levels of screening may occur before the baggage is loaded onto an aircraft.⁹⁸⁰ As was amply demonstrated by the bombings of Air India Flight 182 and Pan Am Flight 103, baggage screening alone, in the absence of passenger-baggage reconciliation, does not provide adequate protection against bombs in checked baggage:

⁹⁷³ Exhibit P-157, p. 85 of 135.

⁹⁷⁴ Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4529.

⁹⁷⁵ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4520-4521.

⁹⁷⁶ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4520-4521.

⁹⁷⁷ Exhibit P-157, p. 85 of 135.

⁹⁷⁸ Exhibit P-157, pp. 85-86 of 135.

⁹⁷⁹ Wallis, *Lockerbie*, p. 31.

⁹⁸⁰ Exhibit P-169, pp. 65-66 of 202; see also Exhibit P-181, p. 4-2, s. 4.5.

Used as an addition rather than an alternative to the matching process, [baggage screening] will add to passenger safety, providing it is effectively implemented using state-of-the-art technology and procedures. It should *never* be a substitute for passenger and baggage matching, just one of the important ingredients in the security mix.⁹⁸¹ [Emphasis in original]

Neither HBS nor passenger-baggage reconciliation is sufficient alone, but together they provide a powerful defence against bombs in checked baggage. As one expert noted:

Good security requires an amalgam of ideas, an amalgam of approaches. If you're going to be truly effective, there is no one way to stop the terrorist.⁹⁸²

The combination of HBS and passenger-baggage reconciliation exemplifies the layered approach required for effective security.⁹⁸³

3.5.1.2 Creation of the Canadian Air Transport Security Authority

In 1985, passenger and baggage screening was an air carrier responsibility, with limited direction and oversight provided by federal authorities. This was one of the major security weaknesses.⁹⁸⁴ Systemic deficiencies contributed to a series of failures in passenger and baggage screening, which allowed a bomb concealed in unaccompanied interlined baggage to be placed on board Air India Flight 182. Security was not the primary concern of air carriers, which contracted with private security firms, often hiring the lowest bidder to provide screening services.⁹⁸⁵ Generally, the customer service department of air carriers, rather than the security division, hired and supervised screening contractors. Transport Canada recognized this shortcoming:

The Passenger Services staff at airports are primarily concerned with facilitation; security and facilitation are often in direct conflict with each other. There have been many cases when Passenger Services staff have put pressures on the contract screening company which is working for them to speed up security and move passengers through the screening process quickly.⁹⁸⁶

⁹⁸¹ Wallis, *Lockerbie*, p. 154.

⁹⁸² Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4258.

⁹⁸³ Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8234.

⁹⁸⁴ Exhibit P-157, p. 115 of 135.

⁹⁸⁵ Exhibit P-157, p. 55 of 135.

⁹⁸⁶ Exhibit P-157, p. 55 of 135.

After the bombing of Flight 182, Transport Canada considered other methods for delivering screening services for passengers and baggage. Ultimately, the Department decided to leave screening with the air carriers, but develop a highly prescriptive regulatory regime and strengthen training programs for screening personnel. It was not until 2002, in response to the September 11, 2001, attacks, that this arrangement was altered. A separate government authority was created, dedicated exclusively to security screening.⁹⁸⁷

On March 27, 2002, the *Canadian Air Transport Security Authority Act (CATSA Act)*⁹⁸⁸ received Royal Assent, and a new Crown corporation, the Canadian Air Transport Security Authority (CATSA) was established. CATSA had broad responsibilities for screening passengers and their carry-on and checked baggage.⁹⁸⁹ In November 2002, the Minister expanded CATSA's responsibilities to include the random screening of non-passengers with access to restricted areas at airports, along with their possessions.⁹⁹⁰ Non-passengers work at airports, provide services or deliver goods to airports, or pass through airports and require access to restricted areas.⁹⁹¹ The *CATSA Act* assists Canada to comply with Annex 17 of the *Chicago Convention*, which requires contracting states to screen all passengers and their carry-on baggage,⁹⁹² checked baggage⁹⁹³ and a proportion of non-passengers with access to restricted areas of an airport.⁹⁹⁴

Section 6(1) of the *CATSA Act* outlines CATSA's mandate:

The mandate of the Authority is to take actions, either directly or through a screening contractor, for the effective and efficient screening of persons who access aircraft or restricted areas through screening points, the property in their possession or control and the belongings or baggage that they give to an air carrier for transport. Restricted areas are those established under the *Aeronautics Act* at an aerodrome designated by the regulations or at any other place that the Minister may designate.

Under the *CATSA Act*, "screening" is defined as "...screening, including a search, performed in the manner and under the circumstances prescribed in aviation security regulations, security measures, emergency directions or interim orders made under the *Aeronautics Act*."⁹⁹⁵

⁹⁸⁷ Exhibit P-157, p. 67 of 135.

⁹⁸⁸ S.C. 2002, c. 9, s. 2.

⁹⁸⁹ Exhibit P-169, p. 16 of 202.

⁹⁹⁰ Exhibit P-169, p. 18 of 202. CATSA is also responsible for implementing the Restricted Area Identification Card (RAIC), which incorporates biometric identifiers for those granted access to restricted areas of airports: see Exhibit P-169, pp. 61, 73 of 202.

⁹⁹¹ Exhibit P-169, p. 18 of 202.

⁹⁹² Exhibit P-181, pp. 4-1-4-2, s. 4.4.

⁹⁹³ Exhibit P-181, p. 4-2, s. 4.5.

⁹⁹⁴ Exhibit P-181, p. 4-1, s. 4.2.

⁹⁹⁵ *CATSA Act*, s. 2.

CATSA provides screening services at 89 airports across Canada designated by Transport Canada,⁹⁹⁶ covering roughly 99 per cent of all passenger traffic. It screens more than 37 million passengers, 700,000 non-passengers and 60 million pieces of luggage annually. More than 4,000 screening officers are employed by private security firms with which CATSA has contracted for screening services.⁹⁹⁷ CATSA is responsible for establishing criteria for the qualifications, training and performance of screening contractors and screening officers. These criteria must be at least as stringent as the standards established in the aviation security regulations made under the *Aeronautics Act*,⁹⁹⁸ and CATSA must certify all screening contractors against these criteria.⁹⁹⁹ CATSA has established detailed Standard Operating Procedures (SOPs) for its screening services, and has developed operational plans for all 89 designated airports.¹⁰⁰⁰

As part of its screening mandate, CATSA manages the acquisition, installation and maintenance of screening equipment.¹⁰⁰¹ It has deployed more than 6,000 pieces of equipment, involving X-ray, Computed Tomography (CT-X) and explosive trace detection technologies for screening carry-on and hold baggage.¹⁰⁰² This equipment is far more advanced than the simple X-ray machines and crude explosives detection devices that were available in 1985, and is capable of detecting prohibited items more quickly and with much greater sensitivity and accuracy.¹⁰⁰³

CATSA does not currently employ its own explosives detection dogs to assist with passenger and baggage screening. One of the main concerns is that such dogs are not trained to interact in a screening capacity with passengers and could pose a danger. CATSA is reviewing the possibility of incorporating the dogs as an added security layer for passenger and baggage screening.¹⁰⁰⁴

In 2006, a report was released by the *CATSA Act* Review Advisory Panel (CATSA Advisory Panel), an independent three-member panel of experts appointed by the Minister of Transport to conduct a five-year review of the *CATSA Act* and CATSA's operations.¹⁰⁰⁵ The report, *Flight Plan: Managing the Risks in Aviation Security*,¹⁰⁰⁶ noted that in CATSA's five years of existence, the organization had "... achieved a great deal when measured against the security situation prior to its

⁹⁹⁶ Exhibit P-169, p. 17 of 202.

⁹⁹⁷ Exhibit P-157, p. 104 of 135.

⁹⁹⁸ *CATSA Act*, s. 8(1).

⁹⁹⁹ *CATSA Act*, s. 8(2).

¹⁰⁰⁰ Exhibit P-157, p. 104 of 135.

¹⁰⁰¹ Exhibit P-169, p. 32 of 202.

¹⁰⁰² Exhibit P-169, p. 160 of 202.

¹⁰⁰³ Exhibit P-157, p. 104 of 135; see also Section 3.6 for a more detailed account of the current technology being used for passenger and baggage screening.

¹⁰⁰⁴ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4825.

¹⁰⁰⁵ Section 33 of the *CATSA Act* directs the Minister of Transport to conduct a review of the legislation five years after its enactment and to report the results to Parliament. On November 23, 2005, the Minister of Transport announced the appointment of a three-member panel of experts to conduct an independent review and to provide its recommendations and observations. See Exhibit P-175, ss. 33(1), 33(2); see also Exhibit P-169, p. 19 of 202.

¹⁰⁰⁶ See Exhibit P-169.

inception.”¹⁰⁰⁷ Among the Panel’s many recommendations,¹⁰⁰⁸ it is notable that no concerns were expressed about the current security measures for screening passengers and their baggage.¹⁰⁰⁹

Experts and stakeholders have identified CATSA as the appropriate authority to take on greater screening functions, including those involving air cargo.¹⁰¹⁰

3.5.2 Passenger and Baggage Security: Lessons Yet to be Learned

3.5.2.1 *Need for Proactive Approach*

Most improvements to passenger and baggage screening occurred only after major aviation security disasters: Air India Flight 182, Pan Am Flight 103 and the terrorist attacks of September 11th. In a consistently reactive process, new layers of screening have been introduced against sabotage by passengers or by bombs in baggage. The effectiveness of these measures has been limited by the technology used and by the skill of security screening staff and their supervisors.

Aviation security, however, must be based on risk management principles¹⁰¹¹ which are proactive and forward-looking, while at the same time providing protection from existing threats. Although aviation security incidents are rare, their consequences can be devastating. The aim is prevention. In virtually every major aviation security incident since 1985, the need for enhancements to passenger and baggage screening was known, or ought to have been known, often well in advance of the occurrence. Complacency and lack of vigilance exacted a price.

A recent pre-board screening (PBS) initiative illustrates the point. In August 2006, a terrorist plot was uncovered in the United Kingdom. It was suspected that explosive liquids and gels would be used to launch a simultaneous attack against several aircraft crossing the Atlantic.¹⁰¹² The threat was considered imminent. Canada, along with others in the international community, quickly implemented emergency security measures. A complete ban on liquids and gels in carry-on baggage was immediately instituted until the risk could be further assessed. It was later determined that limiting the volumes of liquids and gels in carry-on baggage would adequately address the risk and minimize passenger inconvenience. The response was impressive: in a surprisingly short time, the international community successfully coordinated its efforts to deal with what

¹⁰⁰⁷ Exhibit P-169, p. 18 of 202.

¹⁰⁰⁸ Exhibit P-169, pp. 177-183 of 202; see also Appendix D for a complete list of the Panel’s recommendations.

¹⁰⁰⁹ A number of recommendations dealt with improving the ability of screening officers, however, to effectively implement the security screening measures that are in place. See Section 3.7, which provides a detailed analysis of screening officers within the civil aviation security regime.

¹⁰¹⁰ Exhibit P-169, pp. 55, 69 of 202.

¹⁰¹¹ See Section 3.3 for a detailed analysis of risk management principles in civil aviation security.

¹⁰¹² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585.

UK intelligence had exposed as an impending threat to aviation. Since then, limits on the amounts of liquids and gels in carry-on baggage have become a routine PBS security screening measure to prevent sabotage.¹⁰¹³

Transport Canada has frequently cited the rapidity and ultimate success of the response to the liquids and gels threat of August 2006 as an example of the effectiveness of its security regime and of worldwide collaboration in this area.¹⁰¹⁴ Still, emergency measures are never ideal. Measures that are rapidly instituted in emergency situations can generate chaos and confusion and leave room for error. The measures may inadvertently heighten risk. In 2006, the sudden implementation of sweeping screening measures for liquids and gels created an additional security risk. Heathrow Airport in London came to a standstill, with extraordinarily long lines forming at security screening points and throngs of passengers assembled outside terminal buildings. Sabotage aimed at aviation seeks to produce the greatest impact and probes for areas of vulnerability. Crowds of passengers that congregate in less secure areas of an airport create a "target of opportunity."¹⁰¹⁵ Resort to "knee-jerk" emergency measures must be avoided.

The Commission learned that the threat posed by liquids and gels was known long before 2006. Virtually the same threat arose almost two decades earlier. On November 29, 1987, liquid explosives carried in hand baggage resulted in the destruction of Korean Air Flight 858 as it flew over the Andaman Sea, destined for Seoul, South Korea. All 115 people on board were killed.¹⁰¹⁶ Liquid explosives had been disguised as alcohol in a whiskey bottle that was sealed to appear unopened. A portable radio containing the detonator was placed beside it in a duty-free bag, along with a carton of cigarettes. These were items which could easily have been purchased in the duty-free shop and had not aroused suspicion.¹⁰¹⁷ The bag was placed in an overhead compartment on the flight by two passengers, members of the North Korean Workers Party, who boarded at the initial departure point in Baghdad. They disembarked at a scheduled transit stop, purposely leaving the bag behind on the aircraft. The explosives were timed to detonate later.¹⁰¹⁸

Following the Korean Air bombing, the Council of ICAO requested its Committee on Unlawful Interference to advise on any changes required to security procedures for detecting explosive substances and for controlling the movement of transit and transfer passengers. Although the work of this Committee does not normally "lend itself to rapid action,"¹⁰¹⁹ the airlines were monitoring the latest developments in the field of explosive substances, much of which research was conducted through government funding.¹⁰²⁰ By 2006,

¹⁰¹³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5139.

¹⁰¹⁴ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4842.

¹⁰¹⁵ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4508.

¹⁰¹⁶ Wallis, *Combating Air Terrorism*, p. 18.

¹⁰¹⁷ Testimony of Moses Aléman, vol. 36, May 30, 2007, pp. 4269-4270.

¹⁰¹⁸ Wallis, *Combating Air Terrorism*, pp. 18-19.

¹⁰¹⁹ Wallis, *Combating Air Terrorism*, p. 19.

¹⁰²⁰ Wallis, *Combating Air Terrorism*, p. 19.

this well-known threat should have been managed. Instead, the world seemed caught by surprise. As a result, excessive measures were hastily put in place in response to the imminent plot in the UK. Had security screening measures already existed for liquid explosives, the response in 2006 could have simply adjusted to deal with the specific threat.

Rodney Wallis, an expert in international civil aviation security, expressed frustration that the imminent threat of a second incident was required before appropriate measures were implemented:

Now, in the comparatively recent past, we have heard all sorts of things about governments moving quickly on banning liquids in flight. I say moving quickly, [but] we're talking here 1987. 1987 to 2007 is hardly quick...we've had experience with liquid explosives before.¹⁰²¹

The lesson of the threat from liquid explosives ought to have been learned more than 20 years ago.¹⁰²² The CATSA Advisory Panel reasoned that action had not been taken previously "...probably because there was...insufficient political will to impose this new restriction on passengers. With [the] apprehension of this [alleged 2006] plot that will was suddenly there."¹⁰²³ The Commission heard evidence suggesting that threats, such as those exposed by the loss of Air India Flight 182, may not be fully appreciated until they appear to be directed against Western targets.¹⁰²⁴ It is possible that the lack of political will in 1987 can be similarly explained.

As part of a proactive approach to security, Canada must also do its utmost to follow international best practices. Canada complied with the 2006 deadline set by ICAO for implementing full HBS. However, the Annex 17 standards are really minimum standards, since they require the consensus of all contracting states. Nations with the sufficient resources should be able to exceed these standards. The possibility that, in Canada, HBS could have been put in place much earlier cannot be overlooked, particularly because multi-tiered screening of all hold baggage had been conducted in the UK since the 1990s.¹⁰²⁵

The bombing of Pan Am Flight 103 occurred in 1988. In 1990, the UK Department of Transport proposed that the European Civil Aviation Conference (ECAC) adopt full HBS as a standard security measure. However, the proposal met with resistance since many states believed that no existing equipment was capable of performing such a task. The ECAC set full HBS as a strategic objective to be

¹⁰²¹ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4268.

¹⁰²² Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4270.

¹⁰²³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585.

¹⁰²⁴ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4527; see also Sections 3.3 and 3.8 for a more detailed discussion of this issue and the gaps in aviation security which must be closed.

¹⁰²⁵ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4753.

achieved by 2000. ICAO followed suit, setting 2006 as its target date for member states.¹⁰²⁶ Still, there was not full support for immediate action on HBS, except for conducting research. The UK decided to move ahead unilaterally to develop this measure.¹⁰²⁷ The British Airports Authority, responsible for the majority of airports in the United Kingdom, decided that, “rather than be pushed they’d jump.”¹⁰²⁸

The British Airports Authority collected equipment from around the world, largely from the United States, and proceeded to conduct its own experiment at Glasgow’s Abbotsinch Airport, beginning in 1993.¹⁰²⁹ The equipment was installed over the existing baggage belt system and a three-stage system for screening 100 per cent of hold baggage was developed.¹⁰³⁰ The experiment proved successful and, by 1998, equipment was installed in several airports across the UK, including Heathrow Airport in London. This was eight years ahead of the ICAO deadline, primarily using equipment that was available in North America.¹⁰³¹ Although full HBS was possible in the 1990s, Canada did not accomplish this until the 2006 ICAO deadline.

Of note, the HBS process established in the United Kingdom in the 1990s was accompanied by passenger-baggage reconciliation, which meant that those airports using both systems had “the best defences available at the time.”¹⁰³²

3.5.2.2 Holistic Security: “Single Entity” Doctrine

Although comprehensive passenger and baggage screening provides important protection, more is required. The loss of Korean Air Flight 858 exemplified the danger posed by “transit” passengers who board a flight and then disembark at a transit stop.¹⁰³³ Following the Korean Air disaster, the ICAO Council requested its Committee on Unlawful Interference to review security measures for passengers and their hand baggage at transit and transfer points. Just like interlined passengers and baggage, transit passengers and their baggage need to be accounted for:

So it’s the same recurring story, that people are dangerous when they leave things behind. They are dangerous when they separate themselves from their baggage....¹⁰³⁴

¹⁰²⁶ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4750–4751.

¹⁰²⁷ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4751.

¹⁰²⁸ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4751.

¹⁰²⁹ Exhibit P-179, p. 1.

¹⁰³⁰ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4751–4752.

¹⁰³¹ Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4752–4753.

¹⁰³² Testimony of Rodney Wallis, vol. 39, June 4, 2007, pp. 4753–4754.

¹⁰³³ Wallis, *Combating Air Terrorism*, p. 18.

¹⁰³⁴ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4269.

The principle that a passenger and his or her baggage must be considered a single entity emerged from the international discussions in the days following the bombing of Air India Flight 182. One significant outcome of an extraordinary meeting of the Security Advisory Council (SAC) at the International Air Transport Association (IATA) had been the need to accept the “single entity” doctrine: that the danger of an act of unlawful interference arises whenever passengers voluntarily separate themselves from their baggage.¹⁰³⁵ This included “the no show, the transit or online transfer and the interline passenger.”¹⁰³⁶

Extending this concept further, the entire aircraft must be viewed as a single entity, including all persons or things that are permitted on board or that have access to it. A narrow focus on passengers and their baggage belies the nature of aviation terrorism, which probes for weak links in the security chain. The potential exists for a bomb to be placed on board an aircraft in cargo, mail or catering supplies, for example, and by non-passengers who have access to the aircraft. Security measures are not adequate to prevent these methods of sabotage.¹⁰³⁷

Since 1985, Canada’s efforts to enhance aviation security have disproportionately focused on improving passenger and baggage screening, leaving other known vulnerabilities, such as air cargo, undesignated airport facilities and persistent gaps in airport security, unaddressed.¹⁰³⁸ The Standing Senate Committee on National Security and Defence (Senate Committee), which has been reviewing the state of aviation security in Canada since 2002, compared aviation security to a house with a “fairly well secured” front door, but with side and back doors that are “wide open.”¹⁰³⁹ Despite these known deficiencies and the fact that passenger and baggage security has been quite comprehensively addressed since January 2006, with the implementation of full HBS, successive budgets have continued to concentrate funding on passenger and baggage initiatives, perhaps at the expense of other aspects of aviation in need of attention.¹⁰⁴⁰ The 2009 Budget pledged funding for a new air cargo security initiative, but it also announced funding for a new passenger assessment system. It is important that policy decisions in civil aviation security reflect all risks in a balanced manner. It is only within the past five years that Transport Canada has begun to consider strengthening some of the long-known gaps in the aviation security regime, but concrete measures are still to be implemented.¹⁰⁴¹

¹⁰³⁵ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4475-4476.

¹⁰³⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4476.

¹⁰³⁷ See Sections 3.8.1 and 3.8.2, which describe the vulnerabilities in air cargo and airport security in greater detail.

¹⁰³⁸ A 2005 report by the Auditor General of Canada, which reviewed the 2001 Anti-Terrorism Initiative, noted that following the September 11, 2001 attacks, the federal budget had directed aviation security funding only to passenger transportation. See Exhibit P-411, p. 9.

¹⁰³⁹ Exhibit P-171, p. 9 of 256.

¹⁰⁴⁰ Exhibit P-411, p. 9.

¹⁰⁴¹ See Section 3.8, which describes the current major gaps in security and Transport Canada’s plans to address them.

3.5.3 Passenger and Baggage Screening: Current Procedures and Future Developments

3.5.3.1 Hold Bag Screening and Passenger-Baggage Reconciliation

With full HBS, the processing of checked baggage has become more complex, as have the roles and responsibilities of the participants. Baggage is the air carrier's responsibility after acceptance from the passenger at check-in. It is then processed through the airport's baggage handling system to CATSA's HBS operations. Transport Canada has specified various configurations of equipment and screening processes for HBS, depending on the volume of checked baggage that passes through an airport, as well as space limitations.¹⁰⁴² A screening process with up to five levels of in-line equipment, using advanced X-ray and explosives detection technology, has been implemented.¹⁰⁴³ Screening officers review X-ray images from the explosives-detection equipment, looking for potentially suspicious bags. If suspicions about an item cannot be resolved following this process, the bag is opened and inspected by hand with the passenger present.¹⁰⁴⁴

At major airports where the five-level screening process is available, the system can handle about 800 to 1,000 bags each hour. A certain percentage of baggage in this system is cleared by the equipment, but images of bags that have not been cleared are reviewed by one or more screening operators, who typically have 15 to 20 seconds to make a decision. If baggage is not cleared within the time limit, it is automatically sent to the next level of screening.¹⁰⁴⁵ If, at any stage, a screening officer suspects that an item dangerous to civil aviation has been detected, the officer must call for emergency response.

While technology for screening hold baggage has greatly improved, it is still limited by the skill of those doing the screening. The level of skill depends on the initial and ongoing training received, as well as on the quality of oversight. Attention to detail and constant vigilance are key in HBS.¹⁰⁴⁶

If the baggage is cleared, it continues through the airport's baggage handling system and is delivered to the baggage make-up area.¹⁰⁴⁷ Here, baggage handlers record the check-in number of each piece, sort baggage according to intended flights and transfer luggage to the appropriate aircraft.¹⁰⁴⁸

Under the *Air Carrier Security Measures*, air carriers are responsible for passenger-baggage reconciliation to ensure that no baggage is placed on an aircraft if

¹⁰⁴² In some cases, equipment is in full view of passengers, while in other cases it is below or behind the check-in area, out of sight. See Exhibit P-169, p. 65 of 202.

¹⁰⁴³ Exhibit P-169, p. 66 of 202.

¹⁰⁴⁴ Exhibit P-169, p. 66 of 202.

¹⁰⁴⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5156.

¹⁰⁴⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4966-4967; see also Section 3.7, which reviews the challenges in recruiting and training qualified screening officers.

¹⁰⁴⁷ Exhibit P-169, p. 67 of 202.

¹⁰⁴⁸ Exhibit P-169, p. 67 of 202.

the passenger does not board.¹⁰⁴⁹ Passenger-baggage reconciliation can be conducted manually or by electronic systems.¹⁰⁵⁰ Whichever method is used, it is the outcome that is important: reconciliation of passengers and baggage.¹⁰⁵¹ Today, automated systems at some airports electronically link boarding passes with the baggage tags on checked baggage. When bags arrive in the baggage make-up area, the baggage tag is scanned electronically, or in some cases, it is manually recorded and matched with the container in which the bag will be loaded for placement aboard the aircraft. If a passenger fails to board, the airline departure control system will alert the departure gate staff, who then tell the baggage handlers to remove the passenger's baggage from the aircraft.¹⁰⁵²

New technologies will facilitate passenger-baggage reconciliation. For example, radio frequency identification (RFID) technology is being evaluated for use on baggage tags. This technology allows baggage in the hold of an aircraft to be identified quickly when its removal is required.¹⁰⁵³

Although passenger-baggage reconciliation is mandatory and acknowledged by Transport Canada to be "a very basic element of the security system,"¹⁰⁵⁴ there is evidence that air carriers do not always comply. In December 2006, facing a Christmas rush, two air carriers – one Canadian-registered and the other American-registered – violated reconciliation requirements. An administrative monetary penalty of approximately \$6,000 was imposed on each. Although Transport Canada viewed this event as a demonstration of the effectiveness of its enforcement program,¹⁰⁵⁵ the penalty assigned to this very serious security breach seems relatively insignificant. The absence of reconciliation procedures in 1985 caused one of the greatest air terrorism incidents the world has seen. In 1988, a breach of this same security regulation resulted in the bombing of Pan Am Flight 103. There should be no exceptions to the rule requiring passenger-baggage reconciliation on all domestic and international flights. Any infringement should be treated in a manner that reflects the gravity of the potential consequences. Full compliance must be the objective.

IATA noted that advances in reservation system technologies have made it much easier for airlines to identify unaccompanied baggage and subject it to additional screening. Airline departure control management systems can now able automatically "red flag" baggage and reservation irregularities, whereas this previously involved a time-consuming manual process.¹⁰⁵⁶ Although air carriers are in the best position to conduct passenger-baggage reconciliation procedures, the Christmas 2006 incident suggests that there may still be

¹⁰⁴⁹ Passenger-baggage reconciliation is required for all domestic and international flights in Canada. See Exhibit P-157, p. 110 of 135.

¹⁰⁵⁰ Exhibit P-157, p. 110 of 135.

¹⁰⁵¹ Testimony of Georgina Graham, vol. 66, October 25, 2007, p. 8234.

¹⁰⁵² Exhibit P-157, p. 58 of 135.

¹⁰⁵³ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5273-5274.

¹⁰⁵⁴ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4844.

¹⁰⁵⁵ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4844.

¹⁰⁵⁶ Exhibit P-258, p. 10.

occasions where air carriers allow passenger convenience and issues of cost to take priority over vital security measures. Consideration should be given to the best method of achieving compliance with passenger-baggage reconciliation measures.

3.5.3.2 Pre-Board Screening

Pre-board screening (PBS) consists of screening passengers and their carry-on baggage. The *CATSA Act* gives CATSA the mandate to perform this function at screening points, as required under Annex 17 of the *Chicago Convention*. The focus is on detecting prohibited objects that could pose a threat to aviation. These include weapons, improvised explosive devices and incendiaries.¹⁰⁵⁷ As a result of the terrorist threat uncovered in the United Kingdom in August 2006, PBS was expanded to include liquids and gels.¹⁰⁵⁸

All departing passengers must be screened before being permitted to enter the airport departure lounge. Screening points for PBS have been established at all of Canada's 89 designated airports, and this involves a multi-stage process. Boarding passes are checked by security screening officers, and all carry-on baggage is scanned by X-ray equipment. If a suspect item is detected in a carry-on bag, or if a bag is randomly selected, it may be subjected to a physical search or to screening by explosives-detecting trace (EDT) equipment. EDT screening is normally conducted by swabbing carry-on baggage and testing for traces of dangerous chemicals. Passengers pass through a walk-through metal detector (WTMD) archway and, if the alarm sounds or if a passenger is selected at random, he or she may be further searched.¹⁰⁵⁹

As with HBS, a screening officer who detects a suspected dangerous item calls for emergency response. At some airports, doors or barriers at screening points are automatically closed when an alarm is triggered, creating an isolation zone, preventing passengers who have not yet been cleared from leaving the area.¹⁰⁶⁰

Some stakeholders have commented that new technologies for issuing boarding passes through the Internet or from automated self-serve kiosks might increase the risk of dangerous persons getting access to restricted areas and aircraft. Some

¹⁰⁵⁷ Exhibit P-169, p. 63 of 202 and note 5.

¹⁰⁵⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585.

¹⁰⁵⁹ Exhibit P-169, p. 64 of 202. In the United States, trace explosives detection portals, commonly referred to as "puffers," have been used to screen passengers for possible contact with explosive substances. The machines were deployed to airports in 2004 to screen randomly selected passengers, but did not function well in the airport environment. The Transport Security Administration (TSA) has decided to scrap the program because of the unreliability of the equipment when exposed to dirt and humidity and resulting high maintenance costs. Since 2005, maintenance of the machines has cost over \$6 million. See "TSA Scraps Airport Screening Program" *The Associated Press* (May 22, 2009), online: Today Show <<http://today.msnbc.msn.com/id/30875442>> (accessed December 18, 2009) ["TSA Scraps Airport Screening Program"].

¹⁰⁶⁰ Exhibit P-169, p. 64 of 202.

have suggested that boarding pass confirmation or review of other air travel documents should be included under CATSA's mandate to ensure that this takes place before passengers enter the departure area. Currently, air carriers perform this function at baggage check-in (if the passenger checks a bag) and at the departure gate.¹⁰⁶¹ The CATSA Advisory Panel noted that adding such duties to CATSA's PBS responsibilities might become necessary in the future, but would require additional personnel and equipment and, to be effective, would require further training for screening officers.¹⁰⁶²

The CATSA Advisory Panel noted that new technologies will redefine what it means to screen "persons" and "things." Integrated scanning units are being developed that can perform multiple functions, such as detecting metal objects and explosives concealed on a passenger's body, as well as explosives in shoes, without the individual removing outer layers of clothing. This technology may permit passengers to be screened without having to have their carry-on baggage or personal belongings screened separately.¹⁰⁶³

New technology may enhance the overall effectiveness of PBS, but privacy concerns must also be considered. For example, Transport Canada has been conducting a pilot project using backscatter X-ray and millimetre wave technology as an added layer in passenger screening.¹⁰⁶⁴ This technology in effect allows looking under clothing to reveal hidden weapons or other dangerous items.¹⁰⁶⁵ In some instances, the images display a silhouette of the body in a nearly nude state.¹⁰⁶⁶ Transport Canada officials reported that these images will likely be retained for reference in the event that a security breach is subsequently detected,¹⁰⁶⁷ but that the length of time such images would remain in a databank remains unclear. Recognizing that there would need to be specific limitations for retaining this information, officials indicated that any retention period would likely be "only as long as is necessary"¹⁰⁶⁸ to resolve an incident. Transport Canada officials explained that this technology could potentially be used as a primary screening tool, forming part of the multi-level system of screening passengers.¹⁰⁶⁹ The technology would not replace the physical pat-down search, but would provide another tool in the "tool box" of screening measures.¹⁰⁷⁰

¹⁰⁶¹ Exhibit P-169, p. 65 of 202.

¹⁰⁶² Exhibit P-169, p. 65 of 202.

¹⁰⁶³ Exhibit P-169, p. 163 of 202.

¹⁰⁶⁴ Testimony of Jean Barrette, vol. 40, June 5, 2007, pp. 4929-4930. The media has reported that this body-imaging technology is slated to replace the discontinued puffer machines as part of passenger screening in the United States. Privacy concerns have been raised there as well. See "TSA Scraps Airport Screening Program."

¹⁰⁶⁵ Exhibit P-278, Tab 6, p. 3.

¹⁰⁶⁶ Testimony of Jean Barrette, vol. 40, June 5, 2007, pp. 4927-4928; see also Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5134-5135.

¹⁰⁶⁷ Testimony of Jean Barrette, vol. 40, June 5, 2007, pp. 4930-4931.

¹⁰⁶⁸ Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4931.

¹⁰⁶⁹ Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4929.

¹⁰⁷⁰ Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4932.

The Office of the Privacy Commissioner of Canada (OPC) reported that some people find the technology more intrusive than pat-down searches because of the nature of the images. Others consider it less intrusive than the physical contact required in a pat-down search. The OPC recommended that, should these technologies be introduced in Canada, they be used as selectively as possible and that travellers have the option of a physical search.¹⁰⁷¹ Transport Canada officials noted that passengers always provide their consent to be screened under the traditional “no search, no fly” principle.¹⁰⁷² In the face of increasingly intrusive technology, however, this once generally accepted rule may now raise a major dilemma for passengers. An appropriate balance must be struck between the security level being sought and the privacy rights of individuals.

Privacy concerns have also been raised about a pilot project conducted at Calgary Airport. There, one air carrier provided passengers with boarding passes containing a scannable bar code. One purpose of the bar code is to detect forged or fake boarding passes, but personal information is also captured, such as the passenger’s name and flight number, and this is retained until the flight departs. CATSA does not at present collect personal information about passengers and does not know the identity of individuals in an airport. This would change if a decision were made to implement the pilot project across the board. The OPC reported that CATSA has provided its assurance that any such information would be used only in the event of a security incident. The OPC acknowledged that this program could be a helpful security measure if forged or fake boarding passes pose a security risk. However, the OPC questioned the need for collecting personal information from boarding passes.¹⁰⁷³

3.5.3.2.1 Identity Screening Initiatives

The Calgary pilot project appears to be part of a growing trend towards “identity screening.” While PBS has traditionally focused on preventing prohibited objects from being brought onto aircraft, many stakeholders strongly criticized what they consider to be a restricted view of security screening. Many advocated a shift in focus to an individual’s trustworthiness and intent, which, it was argued, would result in better use of limited resources and more appropriately reflect a risk-based decision-making¹⁰⁷⁴ approach to security:

The current aviation screening system is built upon a seriously flawed assumption – that everyone poses a potential threat to aviation security. The truth is that the vast majority of individuals...do not pose any kind of threat...A very small fraction of all passengers actually pose some degree of threat,

¹⁰⁷¹ Exhibit P-278, Tab 6, p. 3.

¹⁰⁷² Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4928.

¹⁰⁷³ Exhibit P-278, Tab 6, p. 4.

¹⁰⁷⁴ See Section 3.3, which discusses the concept of risk-based decision-making in civil aviation security in detail.

but our screening resources are greatly diluted by giving the same degree of physical scrutiny to [every passenger].

...

Another erroneous assumption is that an individual does not pose a threat once they have been successfully screened for objects that could be used as weapons. Such a conclusion for much of the general population may be warranted, but it does not apply to a fanatically dedicated and highly trained terrorist. Physical screening by itself is incapable of keeping terrorists off...airplanes, because it is not designed to identify them.¹⁰⁷⁵

It was contended that an appropriately layered approach to security screening requires examining passengers for hostile intent, while at the same time preventing dangerous objects being introduced on aircraft. The success of such "human-centred screening" relies on the identification of trustworthy individuals and then removing or reducing the scrutiny they receive so that efforts can concentrate on "unknown" or "suspicious" individuals.¹⁰⁷⁶ According to the Airline Pilots Association, International (ALPA), which represents over 60,000 pilots and 39 airlines in North America:

Unless and until the system becomes more human-centred, rather than weapon-centred, we will remain vulnerable to potential hijackings and other aircraft attacks. It is an unfortunate reality that trained terrorists do not need weapons to perpetrate crimes aboard aircraft.¹⁰⁷⁷

Screening that is based on identity is troubling from a privacy perspective, however, because of the potential it creates for increased monitoring and surveillance:

As more agencies collect more personal information about our travelling patterns it will become increasingly easy to track our movements. In addition, identity screening places increased emphasis on the integrity of the authentication documents, potentially leading to the need for greater and more intrusive authentication procedures or for a universal form of identification such as a national identity card. In other words, identity screening can lead to other privacy invasive measures.¹⁰⁷⁸

¹⁰⁷⁵ Exhibit P-252, Tab 1, pp. 5-6.

¹⁰⁷⁶ Exhibit P-252, Tab 1, p. 6.

¹⁰⁷⁷ Exhibit P-252, Tab 1, p. 4.

¹⁰⁷⁸ Exhibit P-278, Tab 6, p. 4.

In addition, where identity is being scrutinized, the potential to infringe constitutionally protected rights exists. Following the September 11th terrorist attacks, several security screening initiatives which address personal identity have either been contemplated or put in place. Currently, CATSA does not conduct any type of identity screening, nor is this part of CATSA's mandate, but stakeholders have named CATSA as an appropriate authority should such screening become a regular component of PBS.¹⁰⁷⁹

Advance Passenger Information and Passenger Name Record

The Advance Passenger Information and Passenger Name Record (API/PNR) Program involves the collection, by government, of personal information relating to all air travellers before their arrival in Canada. The purpose of the Program is to identify passengers or crew members who may pose a risk to security.¹⁰⁸⁰

API consists of information found, for the most part, in a passport or an equivalent travel document, including name, date of birth, gender and citizenship, as well as the passport, visa or alien resident number.¹⁰⁸¹ PNR data is far more detailed and includes an array of personal information about passengers that air carriers collect and store in their reservation systems for their own business purposes.¹⁰⁸² The Canada Border Services Agency (CBSA) has collected API data since October 2002 and PNR data since July 2003,¹⁰⁸³ as a result of amendments to the *Customs Act*¹⁰⁸⁴ and the *Immigration and Refugee Protection Act*.¹⁰⁸⁵ The CBSA retains this information for 3.5 years.¹⁰⁸⁶

In 2004, the enactment of the *Public Safety Act*, 2002¹⁰⁸⁷ brought about amendments to the *Aeronautics Act*. These allowed Transport Canada to require API/PNR data from air carriers in advance of an aircraft's arrival in Canada.¹⁰⁸⁸ The amendments specified up to 34 data elements that Transport Canada can request from airlines,¹⁰⁸⁹ provided that this information has been collected by air carriers in their reservation systems.¹⁰⁹⁰ The data elements include information such as the phone number and address of the ticket holder and the travel agency that issued the ticket, the names of the travel agency and the travel agent that issued the ticket, the method of payment, whether the ticket was paid for by someone other than the ticket holder, the number of checked bags and corresponding baggage tag numbers, meal preferences, class of service,

¹⁰⁷⁹ See, for example, Exhibit P-252, Tab 1, p. 7.

¹⁰⁸⁰ Exhibit P-278, Tab 6, p. 1.

¹⁰⁸¹ Exhibit P-278, Tab 6, p. 1; Testimony of Brion Brandt, vol. 40, June 5, 2007, pp. 4914, 4918.

¹⁰⁸² Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4914.

¹⁰⁸³ Exhibit P-278, Tab 6, p. 1.

¹⁰⁸⁴ R.S.C. 1985, c. 1 (2nd Supp.), s. 107.1.

¹⁰⁸⁵ S.C. 2001, c. 27, s. 148(1).

¹⁰⁸⁶ Exhibit P-278, Tab 6, p. 1.

¹⁰⁸⁷ S.C. 2004, c. 15.

¹⁰⁸⁸ *Aeronautics Act*, R.S.C. 1985, c. A-2, s. 4.81 [*Aeronautics Act*].

¹⁰⁸⁹ See *Aeronautics Act* Schedule for a list of API/PNR data that may be collected.

¹⁰⁹⁰ Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4919.

itineraries and dates such as the dates of booking, travel and ticket issuance.¹⁰⁹¹ Air carriers are required to provide this information electronically before the aircraft arrives in Canada.

Concerns were raised by the OPC when the API/PNR Program was first proposed. The OPC was particularly troubled by the creation of a database containing extensive information on the foreign travel activities of Canadian residents. Under the information-sharing provisions of the *Customs Act*, this information would have been available for a virtually unlimited range of governmental purposes, including law enforcement. Under the *Aeronautics Act*, the sharing of information is more limited. API/PNR data obtained from air carriers may be disclosed to other Transport Canada officials¹⁰⁹² and to other specified government departments.¹⁰⁹³ Disclosure must be for the purposes of transportation security, defined as follows:

“...[T]ransportation security” means the protection of any means of transportation or of any transportation infrastructure, including related equipment, from any actual or attempted action that could cause, or result in,

- (a) loss of life or personal injury;
- (b) substantial damage to or destruction of a means of transportation or any transportation infrastructure; or
- (c) interference with any means of transportation or with any transportation infrastructure that is likely to result in loss of life or personal injury, or substantial damage to or destruction of any means of transportation or any transportation infrastructure.¹⁰⁹⁴

The retention period following any disclosure of API/PNR data is seven days.¹⁰⁹⁵

The OPC reported that some of its concerns were addressed by the short retention period and by limits on the purposes for which the information

¹⁰⁹¹ *Aeronautics Act* Schedule.

¹⁰⁹² *Aeronautics Act*, s. 4.81(2).

¹⁰⁹³ API/PNR data as outlined in the Schedule to the *Aeronautics Act* may be disclosed only to the Minister of Citizenship and Immigration and other persons in that department, the Minister of Public Safety and Emergency Preparedness and persons in the CBSA, the chief executive officer of CATSA and other persons at CATSA, the Commissioner of the RCMP and other designated persons, the Director of CSIS and other designated persons for the purposes of transportation security. See *Aeronautics Act*, ss. 4.81(3), 4.81(4) and 4.82(1)–(12).

¹⁰⁹⁴ *Aeronautics Act*, s. 4.81(0.1).

¹⁰⁹⁵ *Aeronautics Act*, ss. 4.81(6)–(8), 4.82(14).

can be used.¹⁰⁹⁶ The OPC nevertheless maintained that "...the collection and retention of a significant amount of personal information about all air travellers is inherently troubling."¹⁰⁹⁷

There is less control over information that is shared beyond Canada's borders. In late 2001, Parliament enacted Bill C-44, *An Act to amend the Aeronautics Act*, which authorized Canadian air carriers to divulge passenger information to the customs and immigration authorities of foreign states. Information can therefore be reciprocally shared with other countries. Under the Canada-US Smart Border Declaration, the two countries share API/PNR information,¹⁰⁹⁸ particularly with respect to high-risk travellers identified through a jointly-developed risk-scoring mechanism.¹⁰⁹⁹ An automated process for sharing this information was implemented on February 6, 2004, on a "need to know" basis.¹¹⁰⁰

Trusted Traveller Programs

A number of stakeholders believe that Canada should move expeditiously toward implementing registered or trusted traveller programs. These programs allow passengers whose trustworthiness has been established by criminal and security background checks and whose identity can be verified with biometrics to be screened electronically at separate checkpoints, facilitating cross-border travel.¹¹⁰¹ These "pre-cleared" individuals can then cross the border more quickly than others.¹¹⁰²

Such programs already exist. CANPASS Air is a CBSA program that facilitates the entry into Canada of pre-approved, low-risk travellers. These travellers clear customs using their iris as a biometric identifier. The Government of Canada contends that this program enables CBSA officers to concentrate on unknown or high-risk travellers. The program is available to citizens and permanent residents of Canada, as well as to citizens and resident aliens of the United States who have resided in either or both countries for the previous three consecutive years.¹¹⁰³ NEXUS is a broadly similar program. It is a joint Canada-US program open to citizens and selected non-citizen residents of both countries. It involves digital imaging. NEXUS facilitates entry into both countries, whereas CANPASS is only for entry into Canada. Under both programs, extensive personal data is shared during the application process, and background security checks are conducted.¹¹⁰⁴

¹⁰⁹⁶ Exhibit P-278, Tab 6, p. 2.

¹⁰⁹⁷ Exhibit P-278, Tab 6, p. 19.

¹⁰⁹⁸ Exhibit P-278, Tab 26, p. 5, item 8.

¹⁰⁹⁹ Exhibit P-278, Tab 6, p. 2.

¹¹⁰⁰ Exhibit P-278, Tab 6, p. 2.

¹¹⁰¹ Exhibit P-252, Tab 1, p. 7.

¹¹⁰² Testimony of Lindsay Scotton, vol. 72, November 6, 2007, p. 9062.

¹¹⁰³ Exhibit P-278, Tab 23, p. 1.

¹¹⁰⁴ Exhibit P-278, Tab 6, pp. 2-3.

Where personal information is exchanged for a benefit, privacy concerns usually surround the use, collection and safeguarding of this information.¹¹⁰⁵ According to the OPC, the fact that the disclosure of information involved in these programs is voluntary somewhat mitigates the privacy concerns, but caution is still warranted. As these programs expand, a “tipping point”¹¹⁰⁶ is eventually reached whereby people become acclimatized to program requirements and a “new normal”¹¹⁰⁷ is created. It becomes normal to expect that in order to cross the border in a timely manner, significant personal information must be divulged and that the information may be stored in a database maintained by a foreign country. As increasingly intrusive security measures become more acceptable, a reduced expectation of privacy results.¹¹⁰⁸ This calls into question the “voluntary” nature of such programs, since disclosure becomes the general expectation of normal travel. The OPC also expressed concern that individuals enrolling in these programs may not be fully aware of the risks of providing information that may be retained in a database in another country – in this case, the United States.

Behavioural Analysis

A number of stakeholders called for behavioural analysis as an additional pre-board screening measure.¹¹⁰⁹ Such a measure accepts the notion that monitoring passengers for atypical or suspicious behavioural patterns or anomalous behavioural attributes can identify those who may present a risk and who may therefore require more rigorous questioning.¹¹¹⁰ Supporters argued that the additional questioning may make it possible to uncover a terrorist.¹¹¹¹ This method of screening seeks to observe passenger behaviour displayed in the airport environment¹¹¹² or with respect to ticket purchasing. Any assessment or action taken would be based purely on the direct observations of passenger interactions in these situations.¹¹¹³ Proponents contended that behavioural analysis would constitute an added element in the multi-layered approach essential to security.¹¹¹⁴

The events which led to the Air India Flight 182 bombing lends some support to the use of such screening tools, since atypical passenger behaviour was a feature of various interactions with Canadian Pacific Airlines (CP Air). The names on the air tickets were changed just before their purchase; a return ticket was switched to a one-way booking; the tickets were purchased within a few days of the flights; two international tickets were paid for entirely in cash; demands

¹¹⁰⁵ Testimony of Lindsay Scotton, vol. 72, November 6, 2007, pp. 9062-9063.

¹¹⁰⁶ Testimony of Carman Baggaley, vol. 72, November 6, 2007, p. 9064.

¹¹⁰⁷ Testimony of Carman Baggaley, vol. 72, November 6, 2007, p. 9063.

¹¹⁰⁸ Testimony of Carman Baggaley, vol. 72, November 6, 2007, p. 9063.

¹¹⁰⁹ See, for example, Exhibit P-252, Tab 1, p. 7.

¹¹¹⁰ Exhibit P-169, p. 163 of 202; see also Exhibit P-252, p. 7 and Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4595.

¹¹¹¹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4595.

¹¹¹² Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4892.

¹¹¹³ Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4892.

¹¹¹⁴ Exhibit P-252, Tab 1, p. 6.

were made to interline a bag for a flight for which there was no reservation; and when the request to interline was met with resistance, the passenger checking his baggage displayed belligerent behaviour. On June 22, 1985, the passenger known as “M. Singh” appeared at the CP Air check-in counter in Vancouver and loudly insisted that his baggage be interlined to Air India Flight 182, even though the flight from Toronto was overbooked and he did not have a reservation. He was aggressive and bullying towards the ticket agent, who initially refused his request but ultimately relented, contrary to standard industry practice and to CP Air’s own security plan.¹¹¹⁵ According to Dr. Reg Whitaker, Chair of the CATSA Advisory Panel, the behaviour exhibited by “M. Singh” in 1985 demonstrated a “...kind of textbook example of something very, very, very wrong with this individual.”¹¹¹⁶ Had suspicious behaviour been actively monitored in 1985, it is possible that the passenger would have been flagged for greater scrutiny. The decision to interline his baggage in violation of normal security procedures might have been reconsidered, even without knowledge of the heightened threat facing Air India.

On the other hand, the point was made that already proven security measures – passenger-baggage reconciliation and hold bag screening – could well have prevented the bomb from being placed aboard Flight 182.¹¹¹⁷ Abnormal passenger behaviour would have been irrelevant. However, a layered approach to security intends measures to overlap. Redundancies provide the most robust defence against air terrorism so that, if one layer fails, another is in place to address the same threat.¹¹¹⁸ Had behavioural analysis been applied in 1985, the bombing might have been prevented even without passenger-baggage reconciliation:

...I think the point here and why Mr. Singh’s “case” is such a kind of a paradigm is that it also illustrates how passenger profiling could certainly have singled out such an individual... and having singled [him] out, given all the inappropriate and anomalous aspects of this passenger and then subject[ing him] to questioning...would have revealed very quickly, I think, that this was a seriously false...proposition that we were dealing with and therefore they would have gone to the bag, et cetera, et cetera.

So it would be a layer of security that if everything works properly, it’s certainly a good addition to the kind of security we have which is presently directed toward discovering dangerous objects, which is not perfect.¹¹¹⁹

¹¹¹⁵ Exhibit P-436, pp. 17-18, 40.

¹¹¹⁶ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4599.

¹¹¹⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4610; see also Testimony of David Lyon, vol. 40, June 5, 2007, p. 4897.

¹¹¹⁸ Exhibit P-252, Tab 1, p. 6.

¹¹¹⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4610.

In fact, some of the troubling passenger behaviour exhibited by M. Singh in June 1985 is now addressed by surveillance of activities that generally take place before a passenger's arrival at the airport. Ticket purchasing patterns are monitored by the airline industry using tools that were not available 20 years ago. Improved technology has enabled airline reservation systems to flag suspicious transactions and travel patterns, which are then subject to further investigation.¹¹²⁰

Air Canada currently monitors its ticketing system, whether web bookings or direct interactions with its call centres, for unusual transactions and purchasing behaviours. The system has been designed to flag transactions in which certain "security indicators" arise. These include factors such as payment in cash by third parties, one-way bookings and certain travel destinations.¹¹²¹ Although the main concern is fraud and similar criminal activity, the same indicators also serve to identify possible threats to aviation security.¹¹²² Call centre agents have been trained to be attentive to such indicators and to refer any unusual behaviour to their security department.¹¹²³

Monitoring ticket purchasing patterns addresses some behavioural issues related to the Air India bombing. It does not deal with the contention that direct observation of passenger behaviour prior to boarding might uncover hostile intent and prevent an aviation security incident. Certainly, the terrorist attacks of September 11th¹¹²⁴ may argue in favour of behavioural analysis. However, a number of concerns were raised, the most notable being the difficulty in constructing an effective and accurate tool that respects individual rights and is not prone to abuse.¹¹²⁵ Other concerns included: the need for additional resources; the competencies and training required; the choice of personnel to conduct such screening; and the need to establish clear guidelines and processes.¹¹²⁶ Experts and Transport Canada officials alike expressed reservations about proceeding with any such measure without carefully considering all its implications and thoroughly examining the experience in foreign jurisdictions.¹¹²⁷ Brion Brandt, Director of Security Policy at Transport Canada, acknowledged that, although in theory there is merit to observing abnormal behaviour in the airport environment, in practice it is fraught with "thorny difficulties."¹¹²⁸

Despite these misgivings, a behavioural analysis program has already been established in Canada to monitor passengers. Under the Canadian Air Carrier Protective Program (CACPP), armed Aircraft Protective Officers (APOs) providing covert security on selected flights use behavioural analysis when observing

¹¹²⁰ Exhibit P-258, Tab 1, p. 5.

¹¹²¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5243-5244.

¹¹²² Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5243.

¹¹²³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5243.

¹¹²⁴ Exhibit P-35, p. 42.

¹¹²⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4601.

¹¹²⁶ Exhibit P-169, pp. 164-165 of 202; see also Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4892.

¹¹²⁷ Exhibit P-169, p. 65 of 202; see also Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4892 and

Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4822.

¹¹²⁸ Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4892.

passengers in airports and on aircraft.¹¹²⁹ Although specific details of the techniques could not be divulged, the Commission was informed that APOs are trained to observe human behaviour and to recognize atypical reactions to various stimuli, including unexpected changes in the environment.¹¹³⁰ Their behavioural analysis training was designed to take into account the requirements of APO work, such as the need to maintain a covert presence. The Commission was informed that there are a vast number of training programs for behavioural analysis and that methods must be tailored to the specific role.¹¹³¹ As such, the APO program in behavioural analysis might not suit screening officers. APOs perform a different role and operate under different circumstances. They do not function in a PBS capacity; their objective is to intervene in the event of impending grievous bodily harm or a threat to the integrity of an aircraft.¹¹³² APOs are also not subject to the same high traffic volumes and time constraints as CATSA screeners.¹¹³³

The Officer-in-Charge of the CACPP, RCMP Superintendent Alphonse MacNeil, was doubtful that the behavioural analysis program used for APOs could simply be applied to CATSA's passenger screening operations. He suggested, however, that "...there may be another behavioural recognition program that would be of value..."¹¹³⁴

Other countries have employed behavioural observation techniques as a passenger screening tool. Israel, the pioneer in behavioural analysis models, has used such techniques extensively and effectively for some time.¹¹³⁵ The use of behavioural analysis by Israel's national airline, El Al, to avert attempted sabotage is often cited:

We know of one particular case of an aircraft that was going to depart London Heathrow for Tel Aviv...[but] because an Israeli security officer happened to be doing her job by profiling the behaviour of a passenger, they managed to find an explosive device, [which] prevent[ed] that aircraft from taking off and saved hundreds of lives.¹¹³⁶

In Israel, trained front line personnel make initial judgments about a passenger's risk using behavioural observations. This results in the triage of passengers

¹¹²⁹ Known as Aircraft Protective Officers (APOs), these are specially trained RCMP officers whose function is to provide armed air marshal services. See Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8067, 8073, 8087.

¹¹³⁰ The appearance of a uniformed officer, for example, "is a change in the environment that could create some concern for someone...if they're doing something they shouldn't be doing": Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8075.

¹¹³¹ Testimony of Alphonse MacNeil and Greg Browning, vol. 65, October 24, 2007, p. 8086.

¹¹³² Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8079.

¹¹³³ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8086.

¹¹³⁴ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8086.

¹¹³⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4595.

¹¹³⁶ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7967.

into low-, medium- and high-risk streams. Aspects of this approach are being adopted at some airports in Europe. In the United States, Boston Logan Airport has pioneered a similar program that streams passengers according to estimated risk, and the Transportation Security Administration (TSA) has piloted the Screening of Passengers by Observation Techniques (SPOT) program that may be applied at a wider range of US airports.¹¹³⁷

However, one of the most significant concerns raised about using this approach in Canada was the discretion that would invariably be given to front line personnel to form judgments about passengers, and the profound impact that this could have on them.¹¹³⁸ Jean Barrette, Transport Canada's Director of Security Operations at the time of the hearings, noted that behavioural assessment techniques are meant to employ objective evaluative criteria, but cautioned that "a fine line"¹¹³⁹ exists between behavioural criteria and criteria that amount to racial profiling.¹¹⁴⁰ The CATSA Advisory Panel also had "doubts about the science"¹¹⁴¹ and was concerned, in particular, about the potential relationship between behavioural profiling and racial profiling.¹¹⁴²

Given the nature and history of aviation terrorism, behavioural analysis as a passenger screening tool could properly include criteria related to religion, nationality or ethnicity.¹¹⁴³ In 1985, for example, taking into consideration the overall profile of "M. Singh," including the ticketing purchase patterns, the destinations and his highly agitated behaviour at the ticket counter, had he also been "...somebody wearing a turban and appear[ing] to be Sikh at a time when Sikh extremism was the issue...[this] would clearly have been a factor"¹¹⁴⁴ if behavioural analysis was being used at the time. Similarly, aviation currently faces a threat from Islamist extremists "...and, therefore, certain kinds of people from certain parts of the world with certain religious affiliation[s] are more likely to pose a greater risk...that's certainly true."¹¹⁴⁵ The CATSA Advisory Panel noted that with a properly implemented approach, racial, religious or ethnic "profiling" is neither a necessary nor an inevitable outcome.¹¹⁴⁶ In theory, any such screening model would require highly trained personnel with the capability to analyze all behavioural cues without inflating the importance of racial, religious or ethnic dimensions. Care would be needed to avoid using such indicators in the prejudicial exercise of authority.¹¹⁴⁷ Whitaker noted that the difficulty lies in the practical application of the analysis:

¹¹³⁷ Exhibit P-169, p. 164 of 202.

¹¹³⁸ Exhibit P-169, p. 164 of 202.

¹¹³⁹ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4822.

¹¹⁴⁰ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4822.

¹¹⁴¹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4597.

¹¹⁴² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4597.

¹¹⁴³ Exhibit P-169, p. 164 of 202.

¹¹⁴⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4600.

¹¹⁴⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4597-4598.

¹¹⁴⁶ Exhibit P-169, p. 164 of 202..

¹¹⁴⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4600.

...[U]nfortunately, it I think proves difficult in practice to contain that within reasonable bounds. I think one of the things we find is that in practice, those on the front line don't necessarily maintain the appropriate balance and their own prejudices may in fact intrude into the practice of behavioural [analysis].¹¹⁴⁸

The CATSA Advisory Panel noted that the threat environment in some other countries, such as Israel, greatly exceeds anything experienced in Canada. Consequently, there may be more widespread acceptance there of security measures than in Canada. Israel, for example, looks at a number of behavioural aspects, including ticket purchasing patterns, itineraries and particular circumstances, which can include nationality, ethnicity and religion.¹¹⁴⁹ Certainly, any true form of racial, religious or ethnic profiling is "...generally seen as inappropriate, if not illegitimate, in Canada."¹¹⁵⁰ Both public perceptions and civil liberties issues,¹¹⁵¹ including the potential for offending the *Charter*,¹¹⁵² would be need to be seriously considered.

Even Israel, with a behavioural analysis system that has been successfully exported to other jurisdictions, has recognized the potential for violating the rights of individuals and is re-evaluating its system:

...[T]he appropriate authorities have recognized, that complaints...[have] been made for many years by human rights organizations and by Arab and Palestinian and Muslim organizations in Israel that in fact this system operates in a way [that] differentially and prejudicially...often subjects Arab and Muslim passengers to humiliating and degrading searches.... [This] has been in fact recognised and consequently they're trying to adjust their system.¹¹⁵³

Whitaker stated that any focus in Canada on criteria such as religion and race would be a "colossal waste of resources,"¹¹⁵⁴ even apart from concerns over the prejudicial effect of such a focus. He noted that, although the overwhelming concern following the events of September 11th was Islamist extremism, only a very "tiny minority" of the Islamic communities in Canada "...in any way, shape or form pose a threat of being terrorists, of being extremists."¹¹⁵⁵ A program that focused on these criteria would not show effective risk management:

¹¹⁴⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4598.

¹¹⁴⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4595.

¹¹⁵⁰ Exhibit P-169, p. 164 of 202.

¹¹⁵¹ Exhibit P-169, p. 164 of 202.

¹¹⁵² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4597.

¹¹⁵³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4598.

¹¹⁵⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4601.

¹¹⁵⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4601.

And consequently, simply identifying people for special attention on the basis of their religion or their ethnicity, would be an enormous diversion of the kind of attention that [could]...be directed [to] a number of other more pertinent criteria.¹¹⁵⁶

While such criteria as religion and ethnicity might be appropriately considered among many factors, the main concern remains the danger of sliding into a system of racial or religious profiling. Maintaining the appropriate balance is difficult.¹¹⁵⁷

CACPP officials advised that the behavioural analysis methods used by APOs do not include indicators such as race, cultural background or appearance.¹¹⁵⁸ They stated that APOs are specifically trained to avoid unintentional racial profiling.¹¹⁵⁹ They rely on assessing human responses, which, if considered abnormal, might indicate that an individual's circumstances may be suspect¹¹⁶⁰:

...[T]he observations are for behaviours out of the norm and you cannot focus on...race or dress. You focus on the human reaction to changes in the environment.¹¹⁶¹

Yet even the neutrality of purported "objective" criteria can be questioned. A 2006 *New York Times* article described criteria used by US Transportation Security Administration (TSA) behaviour detection officers in the United States.¹¹⁶² The article reported that TSA screening officers were being trained to recognize facial expressions that denote emotions such as fear, which could indicate a cause for concern: "...[F]ear is manifested by eyebrows raised and drawn together, a raised upper eyelid and lips drawn back toward the ears."¹¹⁶³ Such observations would then be tabulated using a point system based on facial reactions.¹¹⁶⁴ In addition to facial expressions, other potentially useful criteria appear to include body and eye movements, changes in vocal pitch and other indicators of stress and disorientation.¹¹⁶⁵

Counsel for the Air India victims' families questioned the objectivity of allegedly unbiased criteria, noting that a person's reaction to changes in the environment might be affected by their background. A reaction might be perceived as "unusual" only because it represents a cultural expression with which the program is unfamiliar. As well, emotions such as fear might be based on an individual's

¹¹⁵⁶ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4601.

¹¹⁵⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4601.

¹¹⁵⁸ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8089.

¹¹⁵⁹ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8089.

¹¹⁶⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8089.

¹¹⁶¹ Testimony of Greg Browning, vol. 65, October 24, 2007, p. 8089.

¹¹⁶² Exhibit P-253.

¹¹⁶³ Exhibit P-253, pp. 3-4 of 5.

¹¹⁶⁴ Exhibit P-253, p. 4 of 5.

¹¹⁶⁵ According to the article, the criteria were based on a state police program that had been used at Boston's Logan International Airport to identify drug couriers. See Exhibit P-253, p. 2 of 5.

past experience – for example, with persons in authority – and not predict the commission of harm.¹¹⁶⁶ The potential for misinterpreting behavioural cues might unintentionally lead to targeting certain groups.

MacNeil testified that airports are international environments and that APOs need to be aware of cultural sensitivities. Without such awareness, they would not be effective. He acknowledged that it is not possible to receive instruction on every culture, but emphasized the holistic approach taken by the CACPP. APOs are trained to assess the overall picture, to look at cumulative factors and not to evaluate any one reaction in isolation. APOs are aware that emotions such as fear may have many causes, and are trained not to overreact so that they can maintain, to the extent possible, their covert positions.¹¹⁶⁷

Dr. David Lyon, Research Chair in Sociology and Director of the Surveillance Project at Queen's University, raised another concern. He advised caution when considering behavioural monitoring that does not deal with a concrete "first order of behaviour," such as a criminal record. Direct observations of human behaviour do not have the strength of "a written record of past activities"¹¹⁶⁸ and so deal with probabilities rather than the certainties provided by something like a criminal record. In behavioural analysis, attempts are made to link certain behaviours with possible malign intent. The aim is to prevent something from happening.¹¹⁶⁹ Lyon saw the use of behavioural analysis for passenger assessment as an example of the application of the precautionary principle, in which it is "...believed that we must act on relatively little evidence."¹¹⁷⁰ He acknowledged that certain kinds of risks may warrant such an approach, but warned that "...we need to take tremendous care when we're talking about mere probabilities."¹¹⁷¹

The Commission heard little evidence about the accuracy or effectiveness of behavioural analysis. The *New York Times* reported that during a nine-month period, behaviour detection officers at Dulles International Airport in Virginia referred several hundred people for further screening out of about seven million departing passengers. Of those referred for further screening, less than ten faced legal charges or follow-up, and, even then, largely for immigration matters, outstanding warrants or forged documents.¹¹⁷²

The CATSA Advisory Panel noted that behavioural analysis can involve a mix of technology and human judgment. The Panel was skeptical about developing technologies and their ability to detect malicious intent. These technologies include voice analysis, which measures stress levels, and physiological response

1166 See the line of questioning put to Alphonse MacNeil and Greg Browning by Raj Anand, counsel for the Family Interests Party: Transcripts, vol. 65, October 24, 2007, pp. 8089-8091.

1167 Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8091.

1168 Testimony of David Lyon, vol. 40, June 5, 2007, p. 4896.

1169 Testimony of David Lyon, vol. 40, June 5, 2007, p. 4895.

1170 Testimony of David Lyon, vol. 40, June 5, 2007, p. 4858.

1171 Testimony of David Lyon, vol. 40, June 5, 2007, p. 4896.

1172 Exhibit P-253, p. 3 of 5.

detectors, which function like polygraph tests.¹¹⁷³ These technologies are based on the principle that fear can be measured by psycho-physiological parameters. The Panel thought it unlikely that any of these technologies would be available in the near future.¹¹⁷⁴ Even if they were to prove practicable, other concerns would no doubt arise about the indicators they claim to detect. For example, the identification of stress could have many innocent explanations, such as stress caused by air travel or the simple fact of being tested for stress indicators. In short, the Panel was not persuaded by the evidence about these technologies and did not recommend them for Canadian airports.¹¹⁷⁵

What is left in behavioural analysis is the exercise of human judgment, which would require “an extensive amount of training”¹¹⁷⁶:

It is one thing to look at the criteria, but it is another thing to train the individuals to recognize the behavioural reaction or traits of an individual. And that is not learned over the course of a two-week training course. This is a combination of theoretical training as well as on-the-job kind of training with proper supervision.¹¹⁷⁷

Whitaker agreed that any kind of behavioural analysis program in Canada would require highly trained personnel capable of recognizing objective behavioural traits and patterns. As discussed, utmost care and vigilance would be required to avoid inappropriate profiling.¹¹⁷⁸ However, experts agreed that certain atypical behaviours could properly be used for analysis in Canada, such as the anomalous purchasing patterns and behavioural interactions seen in Vancouver in June 1985.¹¹⁷⁹ It was also recommended that training should include the proper questioning of individuals who have been flagged for greater scrutiny, which also requires behavioural analysis skills.¹¹⁸⁰

Concerns were also expressed about the practicality of behavioural analysis programs in Canada. While this screening process has been successfully used at Israel’s Ben Gurion International Airport, its volume of passenger traffic is relatively low – only about 30 per cent of the volume of passenger traffic at

¹¹⁷³ The Panel also reported that claims have been made on behalf of remote sensing technologies, such as electromagnetic neurological imaging, but which “sound more like science fiction than realizable technology”: Exhibit P-169, p. 163 of 202.

¹¹⁷⁴ The US TSA has begun testing of an Israeli-designed Suspect Detection System (SDS), which consists of a booth in which a three-minute polygraph is administered through a voice recording in order to discern possible criminal intent. If specific parameters are triggered, a further face-to-face examination is conducted. See Exhibit P-169, p. 163 of 202.

¹¹⁷⁵ Exhibit P-169, pp. 163-164 of 202.

¹¹⁷⁶ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4822.

¹¹⁷⁷ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4822-4823.

¹¹⁷⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4600.

¹¹⁷⁹ Testimony of David Lyon, vol. 40, June 5, 2007, p. 4897; see also Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4599-4600.

¹¹⁸⁰ Exhibit P-253, p. 3 of 5.

Pearson International Airport in Toronto.¹¹⁸¹ Incorporating a full behavioural analysis program at large Canadian airports might require redesigning them. Ben Gurion International Airport, on the other hand, was designed with multiple layers of security in mind. Introducing similar designs in Canada would be costly, and the behaviour analysis program would likely greatly increase the time passengers spend between arriving at the airport and departing on their flights.

Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the Commission hearings, testified that any incorporation of behavioural analysis as a screening tool in Canada required careful evaluation:

...[I]t's a very complex issue. It's complex for policy and legal reasons, and the possible introduction of a behavioural analysis component into the Aviation Security Program is one that we are in the very early days of studying. We are certainly very interested in the experiences that other aviation security authorities have with this approach to aviation security as a possible additional layer that can be brought to the enhancement of security.

But consistent with our overall approach to looking at future enhancements to aviation security, we believe there's a delicate balance that needs to be maintained between effectiveness of security, the efficiency of air transportation and the continuing respect for Canadian values, which include privacy and which include the provisions of our Charter.¹¹⁸²

Barrette testified that visits to other states where such programs have been established showed both advantages and disadvantages. The program at Boston's Logan International Airport was examined to assess how it could be applied in Canada.¹¹⁸³ He stated that that Transport Canada was adopting a wait-and-see approach:

...[I]t is on our radar scope, more on the outside of it, to make sure that we assess that properly. I'm a firm believer that if we look at the present security controls that we have in place right now to do right on-the-ground security, let's wait a little bit of time to see the effect of the added value of [Transport Canada's] Passenger Protect Program as well.

There's a very, very important added value to our security program before we launch head first or knee-jerk react in implementing right away a behavioural assessment system

¹¹⁸¹ Exhibit P-169, p. 165 of 202.

¹¹⁸² Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4821.

¹¹⁸³ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4823-4824.

and adding that as an additional responsibility to the pre-board screener. [This is] an item not to be ignored, but one that requires reflection, careful analysis and monitoring on how this is being implemented around the world....¹¹⁸⁴

Barrette acknowledged the need to respect Canadian rights and values, and the real concern about racial profiling. He stated that any additional layers in aviation security must have a positive impact.¹¹⁸⁵

The current regulatory framework does not allow CATSA to screen individuals on the basis of behaviour or identity. However, the CATSA Advisory Panel stated that the *CATSA Act* is broad enough for CATSA to do this if required.¹¹⁸⁶ The Panel expressed reservations about recommending behavioural analysis because of concerns about the potential infringement of *Charter* rights, the resources available, the rigorous training required and the space requirements at airports.¹¹⁸⁷ Although Israel was cited as a successful example, its circumstances were unique and its geopolitical context was quite different from that of Canada. Such screening in Israel required rigorous, specialized training. The degree of discretion assigned to front line workers in making such judgments could have a serious impact on those targeted. The benefits must outweigh the risks, and in some countries where there were higher baseline threat environments, for example, Israel, such measures may be more acceptable to the public.¹¹⁸⁸ Marriott stated that the overall assessment of the CATSA Advisory Panel about the potential benefits and challenges of behavioural analysis for Canada was "on the mark."¹¹⁸⁹

The Commission notes that funding for a new "passenger assessment system" was announced in the 2009 Budget.¹¹⁹⁰ The Commission does not know the nature of this new security program. If the program does anticipate introducing behavioural analysis, it should do so only after a full and frank discussion. The Commission agrees with the CATSA Advisory Panel that international experiences need to be thoroughly reviewed. As well, carefully planned and controlled pilot projects would need to be conducted in Canada to assess, for example, the accuracy of the technique, the competencies and training required, and the overall efficiency and effectiveness of such screening.¹¹⁹¹ In particular, the possibility of behavioural analysis leading, even unintentionally, to real or perceived religious, ethnic or racial profiling, must be addressed.

¹¹⁸⁴ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4823.

¹¹⁸⁵ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4822.

¹¹⁸⁶ Exhibit P-169, p. 64 of 202.

¹¹⁸⁷ Exhibit P-169, p. 65 of 202.

¹¹⁸⁸ Exhibit P-169, p. 164 of 202.

¹¹⁸⁹ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4822.

¹¹⁹⁰ See Exhibit P-407.

¹¹⁹¹ Exhibit P-169, p. 165 of 202.

Passenger Protect Program

“...too dangerous to fly, but too innocent to be arrested.”¹¹⁹²

On June 18, 2007, Transport Canada launched the Passenger Protect Program (PPP)¹¹⁹³ amid considerable criticism, in large part from privacy and human rights advocates.¹¹⁹⁴ The Program is a form of passenger screening. Its introduction marks the advent of Canada’s first “no-fly” list¹¹⁹⁵ and employs mandatory pre-board screening (PBS) focusing on a passenger’s identity.

The Passenger Protect Program permits the Minister of Transport to deny boarding to any passenger whom the Minister believes poses an “immediate threat to aviation security.”¹¹⁹⁶ Transport Canada describes the Program as an additional layer that addresses the continued threat of terrorism and thereby enhances civil aviation security.¹¹⁹⁷

The Program faced strong opposition since its development was announced in 2005.¹¹⁹⁸ Concerns were raised about:

- the rationale for the Program;
- the lack of transparency in the process by which individuals are selected for inclusion on the no-fly list, known as the Specified Persons List (SPL); and
- the lack of transparency in the process for reconsidering placement on the SPL.

On June 28, 2007, ten days after the Program came into effect, Canada’s privacy commissioners and privacy enforcement officials issued a joint resolution about the Program. Among other demands, they called for the immediate suspension of the Program and its referral to a parliamentary committee for a thorough public review.¹¹⁹⁹ The Program has nevertheless continued. On June 4, 2008, almost a year after its launch, the Minister of Transport issued the first boarding denial under the Program to a young man who had booked an overseas flight departing from Montreal. The denial led to a Federal Court challenge alleging that the Program violates rights to free movement and due process guaranteed under the *Charter*, and that it violates privacy rights.¹²⁰⁰

¹¹⁹² Testimony of David Lyon, vol. 40, June 5, 2007, p. 4858. Lyon was describing the Passenger Protect Program and the effect of placing individuals on the Specified Persons List (SPL).

¹¹⁹³ Exhibit P-278, Tab 13, p. 3, s. 10; see also Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4855.

¹¹⁹⁴ Exhibit P-278, Tab 9, p. 1.

¹¹⁹⁵ Exhibit P-278, Tab 8, p. 1.

¹¹⁹⁶ Exhibit P-278, Tab 14, p. 1.

¹¹⁹⁷ Exhibit P-278, Tab 14, p. 1.

¹¹⁹⁸ Exhibit P-278, Tab 10, p. 1.

¹¹⁹⁹ Exhibit P-278, Tab 9, p. 2.

¹²⁰⁰ Exhibit P-426.

In October 2007, the Office of the Privacy Commissioner of Canada (OPC) strongly criticized the Program for "...the secretive use of personal information in a way that will profoundly impact privacy and other related human rights such as freedom of expression and the right to mobility."¹²⁰¹

Under the Program, Transport Canada generates a list of individuals whom it believes pose an immediate threat to aviation security if they board an aircraft.¹²⁰² Before issuing a boarding pass, air carriers must screen the names of passengers against this list.¹²⁰³ If a passenger's name, date of birth and gender match those of a person specified on the list, the air carrier must contact Transport Canada for a determination by the Minister or an authorized delegate about whether to deny boarding.¹²⁰⁴ If a decision is made to deny boarding, the Minister or authorized delegate issues two "Emergency Directions," one directing the air carrier to disallow boarding of the aircraft and the other directing the passenger not to board.¹²⁰⁵

Rationale for the Program

According to Transport Canada, the Passenger Protect Program was implemented to address the ongoing terrorist threat to aviation security, exemplified by the events of September 11th.¹²⁰⁶ Transport Canada developed the Program to strengthen Canada's approach to aviation security and to complement other layers of screening.¹²⁰⁷ The Program applies to all flights to, from and within Canada.¹²⁰⁸

The Program was developed after the enactment of the *Public Safety Act*, 2002 in May 2004. The Act included provisions to strengthen civil aviation security, among them substantive amendments to the security provisions of the *Aeronautics Act*.¹²⁰⁹ This amendment gave the Minister of Transport new powers:

- Section 4.81 of the *Aeronautics Act* allows the Minister, or a delegate, to require an air carrier or an aviation reservation system operator to provide certain information respecting:
 - Persons on board or expected to be on board a specific flight where there is an immediate threat to that flight; or
 - Any particular person whom the Minister has specified for the purposes of transportation security;

¹²⁰¹ Exhibit P-278, Tab 7, p. 30.

¹²⁰² Exhibit P-278, Tab 14, p. 2.

¹²⁰³ Exhibit P-278, Tab 14, p. 1.

¹²⁰⁴ Exhibit P-278, Tab 13, pp. 3-4.

¹²⁰⁵ Exhibit P-278, Tab 13, p. 8.

¹²⁰⁶ Testimony of Brion Brandt, vol. 40, June 5, 2007, p. 4851.

¹²⁰⁷ Exhibit P-278, Tab 14, p. 1.

¹²⁰⁸ Testimony of Brion Brandt, vol. 40, June 5, 2007, pp. 4851-4852.

¹²⁰⁹ Exhibit P-157, p. 99 of 135.

- Sections 4.76 and 4.77 authorize the Minister, or a delegate, to issue Emergency Directions if the Minister or delegate is of the opinion that there is an immediate threat to aviation security;
- Section 4.82 authorizes the Canadian Security Intelligence Service (CSIS) and the RCMP to access and analyze air passenger information for the purposes of transportation security and to investigate threats to the security of Canada, and to disclose this information under certain conditions to designated persons and federal agencies, air carriers, the Minister of Transport, and to any peace officer for reasons of transportation security; and
- Sections 4.85(1) and (3) prohibit persons who must be screened from entering or remaining in an aircraft or a restricted area unless they permit a screening to be carried out, and prohibit air carriers from transporting a person unless that person has been screened.¹²¹⁰

These provisions were criticized by some groups as being overly broad. In a January 2007 letter to the Minister of Transport, the Information and Privacy Commissioner of Ontario recommended the following changes to the *Aeronautics Act*:

- amending section 4.81 to minimize the data required for collection to that which is necessary for aviation security;
- amending section 4.76 to provide an objective standard such that emergency directions are “reasonably necessary and consistent” with the *Charter*;
- amending section 4.72 to preclude making secret “security measures” which have an impact on civil liberties and human rights, including the right to privacy;
- amending the Act to provide “reasonable grounds” that an individual will cause or is involved in planning violence associated with air terrorism; and
- repealing or amending section 4.82(11) to ensure that personal information is disclosed only when an individual presents a serious threat to transportation security or to the safety of the public.¹²¹¹

Transport Canada officials maintained that the *Public Safety Act*, 2002, underwent substantial parliamentary debate prior to its enactment in 2004, following which Transport Canada undertook to implement the Passenger Protect Program. The OPC was very involved in the public debate preceding the enactment of the Act. At that time, however, the possibility that the new provisions would be used for an initiative such as the Passenger Protect Program was never discussed. The OPC became aware of Transport Canada’s

¹²¹⁰ Exhibit P-278, Tab 13, p. 4; see also Exhibit P-174, ss. 4.76, 4.77, 4.81, 4.82, 4.85(1), 4.85(3).

¹²¹¹ Exhibit P-278, Tab 12, p. 1.

plans for the Program through a newspaper report. Only then did Transport Canada brief the OPC on plans for the Program.¹²¹²

The Privacy Commissioner was troubled by the lack of parliamentary scrutiny of the proposal for the Program during the debate preceding the enactment of the *Public Safety Act*, 2002:

That is of great concern to myself and to other privacy commissioners across Canada, that a program with such far-reaching consequences in terms of individual mobility and individual rights should never have been mentioned specifically in context with the possible uses of the legislation, so that ordinary Canadians and, indeed, reasonably well-informed organizations like my office, in fact, learned about this from a newspaper article.¹²¹³

Transport Canada has asserted that the protection of privacy rights and human rights is a core element of the Program and that, during its development, the Department consulted with stakeholders and civil liberties and ethno-cultural groups, and that it continues to work with the OPC on privacy issues.¹²¹⁴ The OPC agreed that it had engaged in consultations with Transport Canada, but stated that some of its concerns remained unaddressed.¹²¹⁵ In August 2005, the OPC posed 24 questions to Transport Canada concerning the Program. Almost a year later, in June 2006, the OPC received answers. The first and foremost of the OPC questions dealt with the rationale for the Program, asking whether any studies had been conducted to demonstrate that advance passenger information is useful in identifying high-risk travellers. The OPC described as unsatisfactory¹²¹⁶ the answer it received, reproduced here:

The Passenger Protect program proposes to use a watchlist to prevent specified individuals from boarding flights based on practical global experience and risk assessment rather than specific studies. Watchlists are used worldwide to protect the public from the actions of certain individuals. Border agencies, for instance, have stopped numerous dangerous individuals from crossing borders. The [Canada] Border Services Agency uses Advance Passenger Information for air passengers already, to great benefit, to intercept dangerous individuals once a flight has landed in Canada. Passenger Protect will use

¹²¹² Testimony of Carman Baggaley, vol. 72, November 6, 2007, p. 9010.

¹²¹³ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, p. 9011.

¹²¹⁴ Exhibit P-278, p. 5.

¹²¹⁵ Testimony of Carman Baggaley, vol. 72, November 6, 2007, p. 9015.

¹²¹⁶ Testimony of Lindsay Scotton, vol. 72, November 6, 2007, p. 9016.

a limited amount of Advance Passenger Information, with respect to specified individuals, to stop individuals who pose a risk to a flight from boarding the flight.¹²¹⁷

The OPC maintained that this response did not sufficiently address how a “no-fly” list will improve aviation security.¹²¹⁸

In support of the Passenger Protect Program, Transport Canada developed the *Identity Screening Regulations* under the authority of the *Aeronautics Act*. The Regulations, which came into effect on June 18, 2007, outline the screening measures to be carried out by air carriers. Under the original regulations, airlines were required to screen the name of any individual who appeared to be 12 years of age or older against the SPL before issuing a boarding pass, regardless of the method by which a boarding pass may be obtained (the minimum age has now been raised to 18 years). If there is a potential match, the air carrier must verify the individual’s identity by examining government-issued identification. If the verified name, date of birth and gender matches a name on the SPL, the air carrier must inform a Transport Canada officer, who will decide whether the individual poses an immediate threat to aviation security and inform the air carrier whether the individual may board the flight.¹²¹⁹

Advisory Group and Specified Persons List

Under the Program, an advisory group created by the Minister is to assess information regarding particular individuals and provide recommendations to the Minister, or to an authorized officer of the Minister, for the purpose of making decisions about threats to aviation security. Guidelines have been adopted by Transport Canada to assist the advisory group. According to Transport Canada, an individual will be placed on the SPL if that individual’s actions lead to a determination that they may pose a threat to aviation security should they be permitted to board an aircraft. These actions include the following:

- An individual who is or has been involved in a terrorist group, and who, it can reasonably be suspected, will endanger the security of any aircraft or aerodrome or the safety of the public, passengers or crew members;
- An individual who has been convicted of one or more serious and life-threatening crimes against aviation security; or
- An individual who has been convicted of one or more serious and life-threatening offences and who may attack or harm an air carrier, passengers or crew members.¹²²⁰

¹²¹⁷ Exhibit P-278, p. 3.

¹²¹⁸ Testimony of Lindsay Scotton, vol. 72, November 6, 2007, p. 9016.

¹²¹⁹ Exhibit P-278, pp. 2-3.

¹²²⁰ Exhibit P-278, Tab 14, p. 2.

The criteria for inclusion on the SPL are not contained in the legislation or regulations, but are simply provided as public information on Transport Canada's website.¹²²¹ The criteria have been widely criticized as being vague, and seem to be provided as examples, leaving unclear the factors that determine inclusion on the list.¹²²² Lyon warned about reliance on the "precautionary principle" that the SPL entailed:

So we have moved from danger, which is fairly clearly defined and has some legal precedence and legal definition, through risk, where you have to collect information to try to find out something in order to meet that risk in some way, through to precaution. Risk...puts in this case, people into categories or their data into categories. But precaution is based on even less. We don't know exactly what the threats might be and we don't know very much about those who may present risks.¹²²³

And yet, it's believed that we must act on relatively little evidence. And so I think...we're talking about a precautionary principle.

This encourages us to further use new technologies, data mining technologies for example, to try to find out who might be a threat.¹²²⁴

Even though the details of a given threat are not known in advance, and without knowing in all cases the underlying rationale, action is taken:

We don't know, but we believe we must act. And that seems to me to be the, in a sense, the dilemma that we find ourselves in. Because who is on the Specified Persons List? Well, it's people who are an immediate threat to aviation security. So, in other words, these are people who are too dangerous to fly, but too innocent to be arrested. So there's a built-in tension within the SPL.¹²²⁵

Lyon spoke of the need to be aware of the shift away from more classical notions of crime control, where due process and concepts such as presumption of innocence are more established and enjoy greater legal protection.¹²²⁶

¹²²¹ Exhibit P-278, Tab 14, p. 2.

¹²²² See, for example, Exhibit P-278, Tab 6, p. 9.

¹²²³ Testimony of David Lyon, vol. 40, June 5, 2007, pp. 4857-4858.

¹²²⁴ Testimony of David Lyon, vol. 40, June 5, 2007, pp. 4857-4858.

¹²²⁵ Testimony of David Lyon, vol. 40, June 5, 2007, p. 4858.

¹²²⁶ Testimony of David Lyon, vol. 40, June 5, 2007, pp. 4857-4858.

In making its recommendations, the Advisory Group is to assess individuals case by case, using information provided by CSIS and the RCMP. Led by Transport Canada, the Advisory Group consists of a senior officer from CSIS, a senior officer from the RCMP and, as required, other Transport Canada officials and representatives from relevant departments or agencies, with advice provided by the Department of Justice.¹²²⁷

Information from foreign or multilateral intelligence and law enforcement agencies will be vetted for accuracy through CSIS and the RCMP, and the Advisory Group will independently analyze any proposal to include an individual on the SPL.¹²²⁸ A reconsideration process is available for those challenging their denial of boarding. Appeals of decisions made by the Office of Reconsideration are possible.¹²²⁹

The OPC was critical of the dual role played by the RCMP and CSIS in the creation of the SPL. Not only do these agencies provide information about potential candidates for the SPL but, as members of the Advisory Group, they provide input into the decision to add individuals they have identified to the list. Given the significance of the SPL and the potential impact on individuals that could arise from the use of incomplete or inaccurate information, some of which will be derived from foreign sources, the decision to add an individual to the SPL "... should be based on a rigorous evaluation of the information provided by the RCMP and CSIS. However, with these two agencies on the Advisory Group one has to question whether this will occur."¹²³⁰

Transport Canada stated that one result of its collaboration with the OPC is a strict retention and disposal regime for personal information. Any identity information received from air carriers is to be retained only for seven days before being destroyed. Information disclosed by Transport Canada to third parties, such as CSIS and the RCMP, must also be destroyed within seven days. Information that Transport Canada receives from CSIS or the RCMP and other security and intelligence agencies about individuals on the SPL is to be retained, with the approval of the originator of the intelligence, usually for five years following the removal of the individual's name from the SPL.¹²³¹

Reconsideration Process

Individuals denied boarding receive an Emergency Direction that is in force for 72 hours, informing them that the Minister of Transport "...is of the opinion that there is an immediate threat to aviation security or to any aircraft or aerodrome or other aviation facility, or to the safety of the public, passengers or crew members."¹²³² They are referred to the Office of Reconsideration if they disagree with the denial.¹²³³

¹²²⁷ Exhibit P-278, Tab 14, p. 2.

¹²²⁸ Exhibit P-278, Tab 17, p. 10.

¹²²⁹ Exhibit P-278, Tab 17, p. 4.

¹²³⁰ Exhibit P-278, Tab 6, p. 10.

¹²³¹ Exhibit P-278, Tab 17, pp. 11-12.

¹²³² Exhibit P-278, Tab 19, p. 3.

¹²³³ Exhibit P-278, Tab 19, p. 5.

Reconsideration is purely a paper process. The applicant submits a written application outlining the grounds for reconsideration. The Office of Reconsideration assesses the applicant's file and any other information provided by the applicant, "using independent security advisors."¹²³⁴ Additional information may be requested from the applicant. Based on the independent advisor's report, the Office of Reconsideration recommends to the Minister of Transport either to confirm the original decision or to reassess the file. Transport Canada then notifies the applicant in writing. If the reconsideration process confirms the original decision, the applicant may seek judicial review in Federal Court.¹²³⁵

The OPC and other rights groups heavily criticized the reconsideration process for several reasons:

- The criteria for inclusion on the SPL are unclear, making it difficult for an individual to challenge the inclusion;
- There is no indication that individuals will have access to the information used to justify their inclusion;
- There is no oral hearing. The process is conducted by correspondence;
- There is a lack of independent decision making. The final determination after reconsideration is made by the Minister, the same person who made the initial determination;
- No monetary compensation is provided to individuals who have missed flights or have suffered other losses or injuries; and
- The reconsideration process is not set out in the regulations or legislation.¹²³⁶

These issues were raised even before the Program came into effect. In January 2007, the Information and Privacy Commissioner of Ontario called for these shortcomings to be remedied and for the process to be afforded the force of law by way of statutory enactments.

Consequences of Boarding Denials

The OPC expressed concern to Transport Canada about how individuals who are denied boarding may be treated by customer agents and airlines. Other passengers may become aware of the denial of a boarding pass and may make incorrect assumptions about the individual, particularly if the individual is a member of a minority group.¹²³⁷ The consequences of a denial of boarding may be much more damaging, and even dangerous, if the denial occurs in relation

¹²³⁴ Exhibit P-278, Tab 18, p. 1.

¹²³⁵ Exhibit P-278, Tab 18, p. 1.

¹²³⁶ Exhibit P-278, Tab 6, pp. 14-15; see also Exhibit P-278, Tab 11, p. 10.

¹²³⁷ Exhibit P-278, Tab 6, p. 13.

to international flights. Foreign citizens trying to leave Canada may be stranded with no other method of returning home. They would undoubtedly have to inform their country representatives of their inclusion on the SPL. This could subject such individuals to further scrutiny by their home states. Similarly, those denied boarding in a foreign country could be vulnerable and at potentially greater risk of detention.¹²³⁸

More troubling is the prospect of local police forces, both in Canada and abroad, becoming aware that an individual has been denied boarding. Transport Canada immediately notifies the RCMP when an Emergency Direction is issued, and the RCMP may then notify the local police force, which can “take action as required.” In addition, the RCMP can provide sensitive personal information, including the individual’s name, gender, date of birth and the fact that there may be a breach of the peace. In the case of an international flight abroad, the RCMP’s International Liaison Branch in the country of departure will be informed of a denial of boarding and could then inform the local police. The OPC expressed profound concern that such disclosure to law enforcement agencies in other countries might have very serious consequences. At a minimum, such a practice will alert the local police to the individual’s whereabouts, and could lead to monitoring of the individual or, worse, deportation or detention.¹²³⁹

Maher Arar, a Canadian engineer, while in transit in the United States, was deported to Syria, where he was imprisoned and tortured.¹²⁴⁰ Arar has publicly expressed concern about the Passenger Protect Program, particularly that many names on the list are likely those of individuals with a Muslim background.¹²⁴¹

Balancing Security and Rights

Jean Barrette, Director of Security Operations at Transport Canada, advised that all civil aviation security measures must balance three basic and sometimes competing principles: optimal security, industry needs and respect for individual rights, particularly those protected under the *Charter*.¹²⁴²

It is reassuring that respect for individual rights is one of the three “basic pillars”¹²⁴³ to be considered when developing security measures, but Transport Canada did not provide any methodology for balancing these interests. According to the OPC, national security and the protection of the privacy of individuals in Canada need not be seen as trade-offs: “...One value does not necessarily need to be sacrificed in the interest of the other. Both can be achieved with well-designed

¹²³⁸ Exhibit P-278, Tab 6, p. 13.

¹²³⁹ Exhibit P-278, Tab 6, p. 14.

¹²⁴⁰ See “Maher Arar: Timeline” (January 26, 2007), online: CBC <<http://www.cbc.ca/news/background/arar>> (accessed December 18, 2009).

¹²⁴¹ Exhibit P-278, Tab 22, p. 2.

¹²⁴² Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4893.

¹²⁴³ Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4893.

law, prudent policy, and effective checks and balances.”¹²⁴⁴ The OPC offered a series of questions to use in determining whether a given measure is justified:

- Is the measure demonstrably necessary in order to meet some specific need?
- Is it likely to be effective in achieving its intended purpose?
- Is the intrusion on privacy proportionate to the security benefit to be derived? and
- Is it demonstrably less privacy-invasive than other measures that would achieve the same purpose?

Applying this approach to the Passenger Protect Program, the OPC commented:

We do not question the need to enhance aviation security, but it is not clear to us that the PPP is demonstrably necessary, that it is likely to be effective or that it is proportionate to the security benefit. Attempting to answer these questions is difficult because the rationale for the program is not clear. In particular, the notion that there are individuals who pose an imminent threat to aviation security but who have not committed any acts that warrant arrest is difficult to understand.¹²⁴⁵

Acknowledging that its expertise is not in aviation security, the OPC nonetheless offered suggestions for less privacy-invasive security alternatives:

- Checking the baggage of passengers perceived to pose a threat;
- More thorough screening of cargo;
- Greater use of air marshals;
- Improved security awareness training for all airport personnel;
- More rigorous baggage reconciliation; and
- Stricter access controls to sensitive areas.

The OPC further noted the inherent incongruity in denying individuals the right to board a flight, while at the same time permitting them to use other forms of transportation, and to attend events where there are likely to be large numbers of people gathered in one place.¹²⁴⁶ Even the choice of an airport as the location at which denial takes place is questionable, given that the ultimate criteria for denial is that the individual is an “immediate threat to aviation security.” The OPC again emphasized that it is not opposed to stronger security measures,

¹²⁴⁴ Exhibit P-278, Tab 10, p. 2.

¹²⁴⁵ Exhibit P-278, Tab 6, p. 5.

¹²⁴⁶ Exhibit P-278, Tab 6, p. 5.

provided they are effective and balanced, but noted that "...expanding the net of surveillance and gathering more personal information does not necessarily result in better security."¹²⁴⁷

The Passenger Protect Program now faces its first challenge in Federal Court.

Regulatory Amendments

It appears that Transport Canada has already acknowledged some of the shortcomings identified in its original formulation of the Passenger Protect Program. Since implementing the Program in June 2007, Transport Canada has continued to consult with stakeholders and has agreed that the following enhancements are required "to improve facilitation, transparency and compliance":

- Removal of requirement for passengers who appear to be under the age of 18 to present identification (currently, a Ministerial exemption is required);
- Removal of requirement for air carriers to verify name, gender and date of birth at the boarding gate, and requiring that carriers verify name only with government-issued documentation;
- Inclusion of the Restricted Area Identification Card (RAIC) as an acceptable non-government identification document for presentation at the boarding gate;
- Incorporation into the regulations of salient elements of the voluntary Memorandum of Understanding currently signed by carriers;
- Designation of monetary penalties (administrative fines) as a more effective and efficient means to enforce the related regulations.¹²⁴⁸

While these amendments do not address some of the core aspects of the Program about which concerns have been raised – namely the criteria and selection process for inclusion on the SPL and the reconsideration process – they signal a recognition by Transport Canada that changes to the Program are necessary.

3.5.4 Conclusion

Multi-level screening of passengers and baggage is a fundamental component of aviation security. Canada has established an impressive program that provides a robust defence against sabotage by passengers and by devices placed in baggage. However, travellers remain vulnerable to other methods of sabotage, particularly sabotage involving air cargo and mail. Excessive

¹²⁴⁷ Exhibit P-278, Tab 10, p. 1.

¹²⁴⁸ Exhibit P-429.

emphasis on passenger and baggage screening to the exclusion of measures to mitigate other threats is misplaced. A holistic approach to security is required. Adequate measures must be implemented to secure air cargo and to protect both restricted and public areas of airports.

The Commission also notes the growing trend towards identity screening. In considering any such measures, the potential for infringing fundamental rights and freedoms must be properly weighed against the possible increases in aviation security. The use of behavioural analysis has the potential to provide another layer of security, but its effectiveness in practice needs to be thoroughly assessed.

3.6 Use of Technology

Technology continues to play an essential role in aviation security because of ever-increasing passenger volumes, renewed awareness of terrorist threats and the demand for faster and more sensitive screening of passengers, baggage and cargo. The Canadian Air Transport Security Authority (CATSA) has put technology to good use in screening 37 million passengers, 700,000 randomly selected non-passengers and 60 million pieces of luggage at Canadian airports each year.¹²⁴⁹ Today's technology is far more powerful and sophisticated than that of 1985. Still, the crucial lesson from the bombing of Air India Flight 182 is that technology is not infallible. However sophisticated it may be, it is only one component of effective aviation security.

More than 6000 pieces of screening equipment are deployed at airports across the country, including X-ray, computed tomography (CT) and explosives trace detection equipment.¹²⁵⁰ This represents an investment of over \$500 million in state-of-the art equipment. These devices are used for pre-board screening of passengers and their carry-on baggage (PBS) and for screening checked, or hold, bags (HBS) before they are loaded aboard aircraft. At present, 100 per cent of passengers and carry-on bags are screened at Canadian airports for domestic and international departures.¹²⁵¹ As of January 1, 2006, 100 per cent HBS was attained for all domestic and international departures at each of Canada's 89 designated airports.

3.6.1 Technology and Pre-board Screening

Today, as in 1985, PBS involves walk-through metal detector (WTMD) archways and X-ray machines to screen passengers and their carry-on bags.¹²⁵² A passenger approaching a screening point is met by a contracted screening officer authorized by CATSA to search for prohibited items that could pose a threat to aviation security. The screening officer examines the passenger's boarding pass

¹²⁴⁹ Exhibit P-157, p. 104 of 135.

¹²⁵⁰ Exhibit P-169, p. 160 of 202.

¹²⁵¹ Exhibit P-157, p. 104 of 135.

¹²⁵² See Volume Two: Part 1, Pre-Bombing, Section 2.3.3, Over-Reliance on Technology.

and then asks the passenger to place carry-on items on a conveyor belt for X-ray scanning.¹²⁵³ The passenger also places any outerwear along with the contents of his or her pockets, and electronic devices (such as a laptop computer) into a tray, and these are also sent along the conveyor belt to the X-ray machine.¹²⁵⁴

The passenger then proceeds through the WTMD. Modern WTMD scanners are sophisticated, computer-controlled devices that are far more precise and consistent in scanning passengers than those in use in 1985. They can differentiate between quantity and type of metals to a certain degree, such that a passenger with a few coins in his or her pocket will not necessarily set off the machine's alarm.¹²⁵⁵ This helps reduce the number of false alarms. If an alarm does occur, the screener conducts another search using a hand-held metal detector (HHMD) wand to determine the location of the metallic object. This secondary examination is also conducted on randomly-selected passengers. If the metallic items are satisfactorily accounted for, the passenger is cleared and can collect belongings at the other end of the screening point, where the conveyor belt delivers them after they have gone through the X-ray machine. If the metallic items are not satisfactorily accounted for, the passenger may be subjected to a physical search at the screening point in an enclosed private area.

During the PBS process, a passenger's carry-on items are opened and searched further if the screening officer observes a potentially suspicious item in the X-ray image, or if the passenger has been randomly selected for additional examination.¹²⁵⁶ The carry-on items may also be examined using explosives detection trace (EDT) equipment.

3.6.1.1 Dual Energy X-Ray

Unlike the low-powered, low-resolution X-ray machines in use in 1985, the scanning systems in use today employ two X-ray beams at different energy levels, allowing the device to differentiate materials within an object being scanned.¹²⁵⁷ The device can detect inorganic materials such as metals, and organic materials such as explosives. The images are displayed on high-resolution colour monitors and are computer-enhanced so that metallic objects appear highlighted, typically in blue, on the monitor, and potentially dangerous organic materials typically appear in orange or red. The computer software is designed to err on the side of caution, highlighting a range of materials as potentially dangerous to minimize the chances of missing anything truly dangerous.¹²⁵⁸ These computer enhancements make it much easier for screeners to examine the contents of a scanned bag. Future enhancements will increase the optical resolution of the dual energy X-ray equipment, an advance that Nick Cartwright, Director of the

¹²⁵³ Exhibit P-169, pp. 63-65 of 202.

¹²⁵⁴ This stage of PBS is known as "divesture." See Exhibit P-169, p. 112 of 202.

¹²⁵⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5126-5128.

¹²⁵⁶ Exhibit P-169, p. 64 of 202.

¹²⁵⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5081-5083.

¹²⁵⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5087-5088.

Security Technology Branch for Transport Canada, likened to the difference between a standard television and a high-definition plasma television.¹²⁵⁹

Small CTX-ray systems, described below Section 3.6.2, will also become available in future for examining carry-on baggage, bringing a new level of image detail, efficiency, and effectiveness to PBS.¹²⁶⁰

3.6.1.2 Threat Image Projection Systems

One challenge in maintaining effective and thorough airport screening is to avoid the screener becoming bored or distracted.¹²⁶¹ Screeners seldom, if ever, encounter a weapon or other dangerous items in scanned baggage, but this creates the risk that they will become less alert to dangers and less motivated to be thorough, since they do not expect to find dangerous items. A new technology – the Threat Image Projection System (TIPS) – plays an important role in keeping screeners alert during PBS. Cartwright explained how the TIPS system works:

... [T]hey developed, through the use of the computer technology, an ability to impose on the image of the bag or replace an image of a bag with something containing a device, whether it be a weapon or a knife or an explosive device, so that this would allow the screeners an opportunity to find something in the course of their business.

... [I]t's both a training [technique] and a useful sort of motivational technique at the same time. There's nothing more that promotes people's enthusiasm [in] their job than actually being able to succeed. And the systems were set up so that as soon as the operator identified something, they would hit a button, and if it turned out to be one of the synthetic images, they would get sort of a green bar ... that said "Congratulations, you found it. This was a TIPS image. You've done your job, but remember you've still got the real bag to do."¹²⁶²

The TIPS system is relatively new, introduced worldwide only after the attacks of September 11, 2001. Cartwright testified that studies have shown that using TIPS images increases screeners' motivation to do a better job, and gives them

¹²⁵⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5095.

¹²⁶⁰ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5104.

¹²⁶¹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5088-5090.

¹²⁶² Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5089.

valuable experience in identifying dangerous items in baggage. The TIPS system is now entering its second generation, with enhancements based on the lessons learned from the first systems.¹²⁶³

3.6.1.3 Explosives Detection Trace and Explosives Vapour Detection Systems

Explosives Detection Trace (EDT) equipment is present at the end of each PBS X-ray point at Canadian airports for use as needed.¹²⁶⁴ The equipment can detect minute traces of explosives residue on the outside of carry-on or checked baggage. Using this equipment avoids the potential danger posed by opening and searching bags that may contain explosives. A cotton swab or special sheet of paper is wiped along the edges of the object to be tested. This will pick up traces of the residue left behind when an explosive device is prepared and placed in or near the bag.¹²⁶⁵ The swabbed sample is then fed into the EDT device, which analyzes the sample and alerts the screener if any suspect chemicals are detected.¹²⁶⁶ The analysis by the device typically takes about six seconds.¹²⁶⁷ Some EDT devices require that the bag itself be physically inserted into a testing chamber. The device then quickly analyzes air samples from around the bag.

The explosives detectors in use today are much more sensitive and reliable than those used in 1985. They can range from small hand-held units to large desktop and floor units. Each has benefits and drawbacks. For instance, the small units are portable, but less sensitive than the larger systems. In addition, the small units can detect explosive vapours well, but are not as sensitive as larger devices to particulate matter or residue.¹²⁶⁸

EDT equipment must be extremely sensitive but also extremely accurate to minimize false alarms, which decrease confidence in the equipment's reliability. Cartwright testified about the very small chemical differences between a molecule of TNT, a powerful explosive, and a molecule of musk ambrette, a very common ingredient in fine perfumes. These molecules differ by only a few atoms of carbon and hydrogen, and would not have been easily distinguishable in 1985.¹²⁶⁹ Cartwright stated that early vapour detectors frequently gave false alarms when exposed to perfumes based on musk ambrette, and that it took some time to determine why.

¹²⁶³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5096.

¹²⁶⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5125.

¹²⁶⁵ Exhibit P-188, p. 7.

¹²⁶⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4972-4973.

¹²⁶⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5124-5125.

¹²⁶⁸ Exhibit P-188, p. 8.

¹²⁶⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5121-5122.

3.6.1.4 Closed-Circuit Television Monitoring

CATSA also uses closed-circuit television monitoring in its airport screening programs. All PBS lines are monitored by camera so that, in the event of a security breach, the passenger in question can be identified and their picture, which is retained for 15 days, relayed to Canada's major airports if they need to be located and apprehended. Monitoring is also useful when a passenger reports a missing item, since footage from the screening process can help determine what happened. As noted, images from the cameras are retained for 15 days, and they can be stored indefinitely on a CD or DVD if a security event occurs that warrants their retention.¹²⁷⁰

3.6.2 Technology and Hold Bag Screening

Since January 1, 2006, and as required by Annex 17 of the *Convention on International Civil Aviation* ("Chicago Convention"), Canada has been using EDT equipment to screen checked baggage for all scheduled flights departing from its designated airports.¹²⁷¹ The Hold Bag Screening (HBS) process has as many as five stages. This is to ensure that potentially suspicious bags receive increasingly intense levels of scrutiny until their contents can be identified as safe or a threat.

3.6.2.1 Canada's Five-level HBS System

The first screening stage ("level one") is completely automated.¹²⁷² Once an airline accepts checked baggage from a passenger, the bags are scanned using a high-speed Advanced Technology (AT) X-ray machine which uses specialized pattern recognition computer programs to identify suspicious images or shapes. Bags are scanned from different angles to permit an examination from more than one viewpoint.¹²⁷³ The machines can handle a full flow of bags at a major airport, typically between 800 and 1000 bags per hour.¹²⁷⁴

If a bag is not cleared for loading aboard the aircraft during the level one screening, it is forwarded to a screening officer for further examination ("level two"). Like the dual energy X-ray machines used in PBS, the AT X-ray devices used for HBS today are highly sensitive, computer-enhanced devices that produce high-resolution images of a bag's contents, making it easier to identify small objects, such as wires, and view them in fine detail. A screening officer examines the AT X-ray scans of the bag made during the level one screening and will clear it or send it for closer examination. The screener's decision must normally be made in 15 to 20 seconds. The system has a fail-safe feature whereby the bag

¹²⁷⁰ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4816-4817.

¹²⁷¹ Exhibit P-169, p. 65 of 202.

¹²⁷² Exhibit P-157, p. 108 of 135.

¹²⁷³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5092-5093.

¹²⁷⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5156.

is automatically sent for the next level of screening if the screener makes no decision within this time.¹²⁷⁵

Level three screening involves a CT X-ray machine conducting further scans of the bag, obtaining three-dimensional images. The CT X-ray system also has automated detection algorithms that allow the machine to determine whether the bag's contents include anything of concern.¹²⁷⁶ If the bag is not cleared at this point, it is sent to the fourth level screening for examination by another screening officer. Computer enhancements to the image also allow potentially suspect bags to be brought to the screener's attention. The process can be configured so that the screener has a finite time to make a decision or can keep the bag in the machine and take further scans.¹²⁷⁷

If the bag is still considered suspect, it is removed from the X-ray machine for a level five examination. This requires having a screening officer test the bag for explosives traces and open the bag for a manual search. Manual searches are normally conducted while the passenger watches, usually from a separate location via closed-circuit TV.¹²⁷⁸ If this search does not resolve the concern, then the bag is passed on to airport authorities and to the police of local jurisdiction.¹²⁷⁹

The five-level HBS system was designed to place the most sensitive and sophisticated equipment where it would be most effective.¹²⁸⁰ The large number of bags screened at level one is best done by high-speed AT X-ray scanners. The smaller number of bags that are not cleared by this initial screening can be handled by highly sensitive, but slower, CT X-ray systems. The system also reflects efforts to balance risk, level of security, cost and availability of resources.

Scanning equipment with the capacity to screen more than one bag at a time gives the five-level HBS system an efficiency boost.¹²⁸¹ Instead of the line of bags coming to a halt when a bag has to be examined by a screener to determine whether it contains anything of significance, a scanning machine with what is called multiplexing capability can process more than one bag at a time. Each of a series of operators examines a different bag on their monitor. Accordingly, the system is not slowed excessively when a bag is routed to a screening officer from a lower level of HBS.

¹²⁷⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5156.

¹²⁷⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5156.

¹²⁷⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5157.

¹²⁷⁸ Exhibit P-169, pp. 65-66 of 202.

¹²⁷⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5157.

¹²⁸⁰ Exhibit P-188, pp. 14-15.

¹²⁸¹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5093.

3.6.2.2 CT X-ray Systems

These machines operate on the same principle as the CT (or CAT) scans used for medical images, and are based on that technology.¹²⁸² The CT scan can provide a three-dimensional image of a bag and rotate the image in any direction. The screening officer can also examine multiple images of the bag at different cross-sections, which facilitates identifying suspect items. Unlike the dual energy X-rays used for PBS, which produce a two-dimensional image where objects are superimposed over one another, the CT X-rays produce a three-dimensional image.¹²⁸³ This allows the contents of bags to be seen more clearly as individual objects. The CT X-ray machines also feature enhanced automatic detection capabilities, making them even more effective at distinguishing explosives from other objects. However, as noted, CT X-ray systems are relatively slow, typically processing only about 200 bags an hour. A large airport would require bag throughput of at least 1000 bags per hour.¹²⁸⁴ Cartwright testified that he expected new CT systems to be able to handle that flow by 2009.

3.6.3 Access Control

One prominent use of technology at Canadian airports is access control. However, as discussed in Volume Two (Pre-Bombing),¹²⁸⁵ a locked door will not necessarily prevent access to vulnerable areas of an airport, even if the door is protected with a coded lock or sophisticated security system. Airport personnel must also be trained well and instilled with strong security awareness. The evidence before the Commission was replete with examples of carelessness leading to unacceptable breaches of security, such as when the code needed to open a secure door was written on the wall. In 1985, another significant problem was the lack of control over restricted area passes. At Pearson Airport, for example, many thousands of passes were lost, not returned, or could otherwise not be accounted for.¹²⁸⁶ This lack of control over restricted area passes continues today. Dr. Kathleen Sweet, a US-based international civil aviation security expert, testified that some airlines now issue passes that dissolve or turn black after 24 hours for visitors, and after one year for employees.¹²⁸⁷

3.6.3.1 Biometrics

The Restricted Area Identity Card (RAIC) system now employed at major Canadian airports is used to establish three different credentials before a person can enter the restricted area: their identity, their clearance, and their right to be in that area. The RAIC system uses biometrics to establish identity, making fraudulent use of an RAIC card extremely difficult.

¹²⁸² Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5087-5088.

¹²⁸³ Exhibit P-188, pp. 4-5.

¹²⁸⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5096.

¹²⁸⁵ Section 2.4, Security Culture at Canada's Airports.

¹²⁸⁶ Exhibit P-101 CAF0555, p. 4; Exhibit P-457, p. 13.

¹²⁸⁷ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4956-4957.

“Biometrics” refers to methods of identifying individuals based on their unique physiological or behavioural characteristics. These include traits such as fingerprints, but also the unique structures of the human face, hand and eye. CATSA has selected a combination of fingerprints and the iris pattern of the eye for biometric access control systems at Canadian airports.¹²⁸⁸

Biometric information is recorded and used only for those who are not passengers. At present, 100,000 non-passengers are entitled to secure area access at Canada’s 29 Class 1 and Class 2 airports.¹²⁸⁹ Following the security clearance process, a new airport or airline employee who requires an RAIC pass card will have his or her iris patterns and fingerprints recorded. The tissue structure of the iris, the coloured part of the eye, is unique for each person, even identical twins.¹²⁹⁰ A detailed photograph is taken of the employee’s iris and a digitally encoded copy created of the mathematical calculations made from the distinctive patterns within the iris. Similar biometric templates are generated from the fingerprints. This data is then written into the computer chip contained in the RAIC card, and the information is encrypted to protect it against unauthorized access.

A non-passenger seeking to enter a restricted area of the airport establishes security credentials by swiping the RAIC near a smart card reader located at the locked entrance door. Each RAIC card has a unique identifier number that the reader scans and compares to a central database that contains only valid identifier numbers. If the system finds a match and confirms that the RAIC card holder is entitled to access the restricted area in question, the non-passenger is then challenged to prove his or her identity by providing biometric information through undergoing an iris or fingerprint scan,¹²⁹¹ or sometimes both. If the system recognizes a match between the scanned iris or fingerprint and the template stored on the card, entry is granted.

The CATSA Review Panel, the Standing Senate Committee on National Security and Defence, and the Auditor General of Canada have all raised concerns about the use of RAICs at Canada’s airports. These include the need to implement biometric access control more comprehensively and rapidly and in conjunction with an enhanced security awareness culture. The Senate Committee also recommended “geo-fencing,” which monitors each time a person enters and leaves a restricted area to enable tracking of unusual or suspicious movement patterns. These concerns are discussed in greater detail in Section 3.8.2, Airport Security.

Access control devices must also be able to prevent “piggybacking” or “tailgating” – for example, where an individual with valid clearance holds a door to a restricted area open for someone following behind but who lacks clearance

¹²⁸⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5159-5164.

¹²⁸⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5166-5167.

¹²⁹⁰ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5160.

¹²⁹¹ Exhibit P-169, p. 74 of 202.

to enter.¹²⁹² Airports are therefore required to ensure that individuals whose clearance and identity have not been confirmed cannot enter a restricted area. Several systems can do this, including “mantrap” doors that unlock only when both the clearance validation and identity validation process have been completed, and that use optical, infrared or pressure sensors to ensure that no more than one person enters at a time.

3.6.4 Technology: Concerns and Limitations

As promising as these many screening and access technologies are, they also have drawbacks. Technology is costly to purchase, maintain and replace. The advanced CT X-ray machines used for HBS cost \$2 million per unit, for example, and are extremely large. Individual units weigh 18,000 pounds, and are 15 feet long and nearly 10 feet high.¹²⁹³ In addition, screening machines are complex. The need to operate them 24 hours a day means that backups must be available if one malfunctions. Servicing of this equipment is generally lengthy and expensive.¹²⁹⁴ There is also strong pressure to upgrade equipment as newer, more effective models become available – bringing additional expense for the equipment itself and for the training to operate it.

Sweet testified technology is an important component of aviation security, but it cannot be its “saviour.”¹²⁹⁵ It was essential to use all available tools, along with common sense, and to avoid the temptation to “fight the last war” at the expense of preparing for the next potential threat.

It is also important to adopt preventive strategies, such as implementing access control systems and regular security patrols for vulnerable areas of the airport. Sweet gave the example of airport fuel depots, which are not necessarily secure or monitored, and could easily be a target for terrorists. She testified that, while recently on a plane leaving Pearson Airport, she saw the gate to the fuel depot open and unprotected.¹²⁹⁶ Compared with the technology for screening passengers and baggage, proper security protection for such areas would be relatively inexpensive and would provide badly needed additional layers of security on the ground. Rodney Wallis, former Director of Security at IATA, also testified that an emphasis on perimeter security and access control at airports “would be right at the top of the list” of priorities for security enhancement.¹²⁹⁷

¹²⁹² Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5167-5168.

¹²⁹³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5100.

¹²⁹⁴ Exhibit P-169, p. 161 of 202.

¹²⁹⁵ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4940-4941.

¹²⁹⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4942-4943.

¹²⁹⁷ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5000-5001.

3.6.4.1 Privacy and Safety Issues

As discussed in the CATSA Advisory Panel report, *Flight Plan: Managing the Risks in Aviation Security*, backscatter X-ray is an emerging technology that has been put into trial service at some US and UK airports to help detect concealed weapons and substances on individuals at screening points.¹²⁹⁸ Backscatter X-ray machines involve rapidly passing a single, low-energy X-ray beam over the body of the person being scanned. The X-rays penetrate clothing but not skin. As a result, the process produces a highly realistic image of the passenger's body under their clothing. Accordingly, the nearly nude image reveals any organic or inorganic objects, such as weapons, explosives or narcotics, concealed on the passenger's body. In her testimony, Sweet bluntly referred to the image as "idiot proof," since any foreign objects would be immediately obvious to a screener seeing the image of an otherwise naked body.¹²⁹⁹

The privacy implications of such technology are obvious, as passengers would be subjected to an intimately revealing search. In the UK, one solution is to give passengers a choice between undergoing the backscatter X-ray where the images are viewed by a screening officer of the same sex, and being frisked by hand.¹³⁰⁰ Manufacturers are working at enhancing "modesty filter" software so that the system more appropriately masks private areas of the body. Another technique is to have the image reviewed by someone in a remote location who cannot actually see the person being screened, so will be unable to identify the person later. The person in the remote location can simply notify a screener at the screening location that an additional search of the person may be required, and why – for example, an object in the person's pocket.

Others are concerned about the potential health consequences for passengers being subjected to a dose of radiation each time they are scanned with backscatter X-rays.¹³⁰¹ Even if the process is safe for the general population, there are concerns about whether pregnant women should be subject to these scans.¹³⁰² Transport Canada states that the radiation levels of a single scan are very low, even less than the dose one would be naturally receiving at cruising altitude.¹³⁰³ However, before such systems are routinely used in Canadian airports, privacy and health and safety concerns must be addressed carefully.

The use of radio-frequency identification (RFID) tags at airports to gather information about passengers raises further privacy issues. For example, a pilot project that began at Calgary Airport on June 20, 2007, used RFID tags embedded in boarding passes to track passenger traffic and wait times.¹³⁰⁴

¹²⁹⁸ Exhibit P-169, p. 162 of 202.

¹²⁹⁹ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4971-4972.

¹³⁰⁰ Exhibit P-169, p. 162 of 202.

¹³⁰¹ Exhibit P-169, p. 162 of 202.

¹³⁰² Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4971-4972.

¹³⁰³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5129-5130.

¹³⁰⁴ Exhibit P-278, Tab 20.

Jennifer Stoddart, the Privacy Commissioner of Canada, testified about the privacy implications of a pilot project in the UK that, like Calgary Airport, incorporated an RFID tag in boarding passes.¹³⁰⁵ In the UK pilot project, the RFID tag would be scanned by sensors located throughout the airport, making it possible to track a passenger's movement constantly.¹³⁰⁶ Besides locating passengers who had not reported to their flight by the time it was ready for departure, the information obtained through these RFID tags could be used by retail establishments to advertise their products based on passenger movement patterns and time spent in line-ups and at retail locations. Stoddart testified that these systems require much more transparency. Passengers should be informed in advance of the uses of the information collected, and which agencies and businesses will have access to it. For the Privacy Commissioner, informed consent was important. She also expressed concern about potential leaks or misuse of this data.¹³⁰⁷

3.6.4.2 Reliability

In its report, the CATSA Advisory Panel stated that, despite all the novel and even revolutionary advances brought to screening technologies by private sector research and development, the impetus for technological solutions has resulted in the marketing of devices whose reliability and usefulness were at best dubious.¹³⁰⁸ Volume Two (Pre-Bombing)¹³⁰⁹ cites the example given by Cartwright in his testimony about the "ALPHA Molecular Locator."¹³¹⁰ This device was useless. It did not even contain any working electronics. The undue faith that Air India placed in the "PD-4" explosives detection device is an even more poignant example of the risks posed by failing to evaluate claims by manufacturers about the effectiveness of a device. The Panel emphasized the importance of the Government being able to objectively assess such claims.¹³¹¹

Some devices produce excellent results in laboratory conditions but are less effective in practice. For example, trace explosive detection portals, also known as "puffer" devices, are designed to identify individuals who are carrying or have been exposed to explosives. These machines feature a walk-through portal that blows air over the passenger's entire body, releasing particles clinging to clothing or the body. The air and any dislodged particles are then drawn into the machine for analysis.¹³¹² These devices have been deployed at airports in some countries, including the US, but have been fraught with reliability problems, particularly "false positives" which erroneously detect evidence of

¹³⁰⁵ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, pp. 9066-9070.

¹³⁰⁶ See the discussion of the RFID project in the Testimony of Georgina Graham, Vol. 66, October 25, 2007, pp. 8232-8234.

¹³⁰⁷ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, p. 9064.

¹³⁰⁸ Exhibit P-169, p. 162 of 202.

¹³⁰⁹ Section 2.3.3, Over-Reliance on Technology.

¹³¹⁰ As briefly described with manufacturer's claims in Exhibit P-188, p. 22.

¹³¹¹ Exhibit P-169, p. 162 of 202.

¹³¹² Exhibit P-169, pp. 160-161 of 202.

explosives.¹³¹³ These false positives and other reliability problems are largely caused by common contaminants found in airports, such as dust, dirt and fuel vapours.¹³¹⁴ The puffers also do not work quickly enough for primary screening, and are better suited for when a passenger is selected for a secondary search.¹³¹⁵ While this technology has potential, Sweet testified that its reliability was not yet any greater than that of explosives detection dogs, which she said are far less expensive.¹³¹⁶

The EDT document scanner is an emerging detection system based on EDT technology. The scanner works on the principle that an individual who handles explosives becomes contaminated by particles of explosive residue and that these particles will spread to other items that the individual routinely handles and carries, including boarding passes and passports. The EDT document scanner examines these documents, which individuals must present before boarding an aircraft. Despite its promise, the reliability and effectiveness of this technology has not yet been clearly demonstrated, and other obstacles remain. For instance, boarding passes are often printed on thermally treated paper, which will turn black if run through a conventional EDT document scanner, making the passes unusable.¹³¹⁷

Devices to detect liquid explosives are another example of rapidly evolving technology. Manufacturers are working to develop quick, affordable, reliable and easy-to-use systems that can scan bottles and other containers during PBS. Some systems are already being deployed, but have limitations. The CATSA Advisory Panel gave the example of a device that uses a laser beam to scan liquids inside clear bottles, but which cannot see through opaque containers.¹³¹⁸ Also, the systems must scan one bottle at a time, making it impractical for large scale use.¹³¹⁹ The value of these systems for aviation security is therefore limited.

Future screening systems may measure a passenger's voice and physiological responses for signs of stress and other indicators that may signify a malicious intent.¹³²⁰ These as-yet-unproven systems would integrate behavioural analysis into the screening process, aided by the judgment of a screener questioning the passenger and examining the computer's results. One system under development, the Suspect Detect System (SDS), consists of a booth in which the subject is given a three-minute polygraph assessment. Over the three-minute period, voice analysis is used to detect indications of fear, on the principle that the indications could signal the apprehension of someone intending to commit

¹³¹³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5118-5119.

¹³¹⁴ Exhibit P-169, pp. 160-161 of 202. These reliability problems prompted the US Transportation Security Administration (TSA) to phase out their use. See "TSA Scraps Airport Screening Program" *The Associated Press* (May 22, 2009), online: MSNBC <<http://today.msnbc.msn.com/id/30875442/>>

¹³¹⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5120-5121.

¹³¹⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4973.

¹³¹⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5151-5123.

¹³¹⁸ Exhibit P-169, p. 161 of 202.

¹³¹⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5136-5137.

¹³²⁰ Exhibit P-169, p. 159 of 202.

a criminal act.¹³²¹ If these indications were detected, the subject would be sent to a face-to-face interview for further scrutiny.

The CATSA Advisory Panel also referred to even more speculative technologies that rely on electromagnetic neurological imaging to “read” areas of the brain that might reveal suspicious intentions, but regarded such technologies as little more than science fiction.¹³²² It is likely that not all these technologies will be shown to be effective, viable security tools in the near future. Even if they did function with acceptable accuracy, the privacy concerns posed by devices that require measurements of speech and physiological indicators such as heart rate or blood pressure will be difficult to resolve. The Panel was not persuaded that these systems should be developed for use at Canadian airports.¹³²³

3.6.5 Other Screening Systems

3.6.5.1 Passenger-Baggage Reconciliation

Passenger-baggage reconciliation is now required for all domestic and international flights departing from Canadian airports.¹³²⁴ This means that checked bags cannot be placed aboard an aircraft unless the owner travels on that aircraft.¹³²⁵ Passenger-baggage reconciliation is required of all air carriers under the authority of the *Air Carrier Security Measures* regulations, and is either done manually or through an automated computer system. This measure would not thwart a terrorist who boards a flight bent on suicide, but it remains an essential and highly effective component of aviation security in other situations.

Technology plays an important role. It is possible to implement such a system without any technological assistance – for example, by placing bags on the tarmac and requiring passengers to identify their bags before boarding, but doing reconciliation without technology would be time-consuming and nearly impossible at a large, modern airport that serves thousands of passengers daily. As well, some manual methods of reconciliation, such as making note of a checked bag’s sequencing number, are subject to human error. Yves Duguay, Senior Director of Air Canada Security and Chair of the IATA Security Committee, testified that Vancouver International Airport and Toronto’s Lester B. Pearson International Airport now scan baggage bar codes to permit computerized tracking.¹³²⁶

Duguay testified that the aviation industry is also considering using baggage tags equipped with RFID chips. This would promote even greater efficiency in the passenger-baggage reconciliation process and, just as importantly, make

¹³²¹ Exhibit P-169, p. 159 of 202.

¹³²² Exhibit P-169, p. 159 of 202.

¹³²³ Exhibit P-169, p. 160 of 202.

¹³²⁴ Exhibit P-157, p. 110 of 135.

¹³²⁵ Exhibit P-169, p. 155 of 202.

¹³²⁶ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5273-5274.

it easier to locate a specific bag in the aircraft's hold whenever it becomes necessary to offload a bag.¹³²⁷

3.6.5.2 Explosives Detection Dogs

CATSA does not use explosives detection dogs for the routine examination of carry-on or checked baggage. Dog teams are funded under contract by the airport authority or provided by the police force having jurisdiction at the airport.¹³²⁸ As in 1985, explosives detection dogs are available at airports for instances of enhanced risk when a bag is considered suspicious following the PBS or HBS process, or when an unattended bag or package is found at the airport. Dogs are also used when there is a need to search an aircraft, in which case hand-held detection devices are also used. Dogs are also used if a suspect vehicle is parked outside the airport and the driver cannot be located.¹³²⁹ Explosives detection dogs are available 24 hours a day at Class 1 airports, such as Toronto's Lester B. Pearson International Airport or Vancouver International Airport.¹³³⁰

Wallis testified that, in his experience, many security experts would rather have a good explosives detection dog than a multi-million dollar piece of equipment.¹³³¹ He testified that dogs have a significant role to play in civil aviation security, and recommended that CATSA screeners have the authority to call for the dogs when needed.¹³³²

Duguay testified that new technologies are being developed to screen large amounts of cargo and are evolving quickly, but explosives detection dogs are also being explored to screen cargo.¹³³³ He stated that explosives detection dogs are increasingly popular in Europe; Lufthansa, for example, is very interested in making greater use of dogs to check cargo. Other countries such as Colombia frequently use explosives detection dogs at airports and for checking vehicles and baggage at hotels. An explosives detection dog team costs about \$100,000 a year, much less than the multi-million dollar cost of some screening devices.¹³³⁴

Similarly, Sweet testified that the small investment required to deploy explosives detection dogs for cargo and baggage brings long-term benefits for airport and aircraft security:

Incredibly, \$10,000 to train them; they'll last for a good 10 to 12 years. Have a good trainer – a good handler, and that dog is good. Those dogs are good. You know, they can sniff out,

¹³²⁷ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5273-5274.

¹³²⁸ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4773-4774.

¹³²⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5220-5222.

¹³³⁰ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4792.

¹³³¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5006.

¹³³² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5014.

¹³³³ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5259-5260.

¹³³⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5110-5112.

what, 5,000 to 7,000 different chemicals, organic compounds or more. Use dogs.

...

Use them on a random basis or you could do individual risk assessments on particular aircraft; maybe aircraft ... going from Canada to a particular area that you might consider dangerous or a little bit riskier, or just randomly.... T]heir appearance sometimes is a deterrent as well, just walking around, seeing them walking through and they stop and sniff your bag, you know, maybe they smell something....

...[T]hey have an attention span ... [of] 20 minutes, then you've got to give them a rest and then put them back on 20 minutes and then give them a rest and put them back on. But ... they don't cost millions of dollars and they are so effective. So effective. And I think that's another way to spend money wisely.¹³³⁵

3.6.6 Conclusion

Technology has improved considerably in recent decades and has proven to be of great assistance in aviation security. Promising new technologies are around the corner. Still, there is a constant danger of placing too much reliance on technology. Devices used for screening passengers and baggage often require skilled operators. A determined terrorist can easily obtain the information and supplies to create powerful explosives in a kitchen or garage.¹³³⁶ These individuals will try to exploit weaknesses in aviation security. It is vital to develop new strategies and technologies to anticipate future tactics to avoid detection of dangerous substances and devices.

Effective security must not focus solely on the "last war" fought. It demands creativity and innovation as well as continued efforts to protect against tactics used successfully in the past.¹³³⁷ No single security system can be completely effective and reliable in every situation. Multiple layers of security, including built-in redundancies, must be incorporated into any security program.¹³³⁸ In this way, the likelihood that a security threat will slip by unnoticed can be minimized, since someone who manages to evade one layer of security will very likely be caught by another. As well, the security value of low-cost, low-technology techniques, such as those involving human skills and canine units, though not infallible, must not be underestimated.

¹³³⁵ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4954-4955.

¹³³⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5131-5133.

¹³³⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5231.

¹³³⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4637-4638.

3.7 Screeners

The Canadian Air Transport Security Authority (CATSA) was created as a Crown corporation on April 1, 2002.¹³³⁹ Key among the security functions assigned to it was responsibility for screening passengers and baggage. The *Canadian Air Transport Security Authority Act* (CATSA Act) defines CATSA's mandate as taking action to provide effective, efficient, and consistent screening across Canada of persons who obtain access to aircraft or airport restricted areas through screening points, as well as of their belongings and baggage.¹³⁴⁰ This responsibility includes random screening of non-passengers, such as airport employees, who access restricted areas.¹³⁴¹ CATSA has jurisdiction at 89 airports across Canada and is funded through an annual budget that must be reviewed by Transport Canada and approved by the Treasury Board.¹³⁴²

CATSA's uniformed screening officers are a familiar sight at airport security checkpoints. They conduct pre-board screening (PBS) of passengers and their carry-on bags and belongings. They also perform hold-bag screening (HBS) and non-passenger screening (NPS). These duties are described in detail in Section 3.5.¹³⁴³

At any given PBS checkpoint, five screening officers are normally present, each with a different duty.¹³⁴⁴ The first screener greets travellers and inspects boarding passes. The second operates the X-ray machine to inspect carry-on items. The third searches carry-on bags. The fourth operates Explosives Detection Trace (EDT) equipment, and the fifth operates the walk-through metal detector and/or the hand-held metal detector. If fewer than five screeners are available to staff a checkpoint, some duties are combined.

All carry-on bags must be X-rayed during PBS and all passengers must clear the metal detector search before being permitted to board an aircraft.¹³⁴⁵ In addition, random searches are conducted of X-rayed carry-on bags and passengers who have cleared the walk-through metal detector, so that the screening officers in these positions are "continuously busy."¹³⁴⁶ EDT screens are conducted both randomly and when the X-ray operator identifies a potentially dangerous item.

¹³³⁹ Exhibit P-169, p. 16 of 202.

¹³⁴⁰ CATSA Act, ss. 6(1), 6(2).

¹³⁴¹ Exhibit P-169, p. 17 of 202.

¹³⁴² The CATSA Act Review Advisory Panel (CATSA Advisory Panel) expressed concerns about the impact of the inflexible budgeting process on CATSA's ability to perform its mandate: See Exhibit P-169, pp. 152-153 of 202.

¹³⁴³ Passenger and Baggage Screening.

¹³⁴⁴ Exhibit P-173, pp. 29-30 of 64.

¹³⁴⁵ Exhibit P-173, p. 30 of 64.

¹³⁴⁶ Exhibit P-173, p. 30 of 64. "Continuously busy" is defined as carrying out the necessary screening of a passenger or bag as per the Standing Operating Procedures, then moving on to the next randomly selected passenger.

Since January 1, 2006, all checked bags for flights departing Canadian airports have been screened with EDT equipment.¹³⁴⁷ HBS is accomplished through multiple layers of scrutiny that balance the automated detection capabilities of state-of-the-art equipment with human skill and judgment. The layered approach to HBS is discussed in detail in Sections 3.5 and 3.6.¹³⁴⁸ Screening officers are located throughout the HBS system, which is designed to inspect bags rapidly but also to err on the side of caution. Bags that cannot be quickly cleared by the computer-controlled detection equipment or by a screening officer are held for further examination.¹³⁴⁹ If a screening officer suspects that a bag contains an item which poses a threat to aviation, such as an explosive device, the officer must call for an emergency response.¹³⁵⁰

Airport operators are responsible for physical access control, such as through installation of doors that can be opened only with a Restricted Area Identification Card (RAIC).

CATSA screening officers perform NPS at airports. This screening is conducted randomly.¹³⁵¹ NPS can be done in several ways, including screening individuals with hand-held or walk-through metal detectors, checking bags and tools with X-ray or EDT equipment, or both. A non-passenger who refuses a search is denied entry to the restricted area. The CATSA Act Review Advisory Panel (CATSA Advisory Panel) recommended expanding NPS.

3.7.1 Recruitment

Several factors affect the staffing of screening officer positions, including competitive job markets for potential applicants, lengthy delays in obtaining security clearances for screeners and the loss of existing screening officers to other jobs. Difficulties in recruiting screeners may lead to practices that increase security risks, among them:

- having too few screeners available during peak periods;
- increasing the use of overtime, which may lead to fatigue;
- deploying staff who lack proper security clearances; and
- shifting staff between NPS and PBS duties.

There is also an ongoing need to “overhire” – hire more employees than strictly needed for existing openings, due to the high turnover rates.

The CATSA Act permits CATSA to provide front line screening services at airports in three ways. The first involves CATSA employees providing screening

¹³⁴⁷ Exhibit P-169, p. 65 of 202.

¹³⁴⁸ Passenger and Baggage Screening; Use of Technology.

¹³⁴⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5156.

¹³⁵⁰ Exhibit P-169, pp. 66-67 of 202.

¹³⁵¹ Exhibit P-169, p. 67 of 202.

services directly. The second involves the use of independent service providers contracted by CATSA. The third has airport operators provide the services, either directly or through contractors.¹³⁵² Since CATSA's inception, contracted service providers have performed its screening functions. CATSA now has more than 20 contracts with 12 organizations for screening services at Canada's 89 designated airports.¹³⁵³ The contractors hire and deploy the screening officers. About 4400 screening officers are deployed across Canada, screening 37 million passengers each year.

Contracting service delivery is less expensive than relying directly on CATSA employees. The CATSA Advisory Panel estimated that moving away from contracted screening services to using CATSA employees as screeners could cost about 40 per cent more.¹³⁵⁴ The Panel concluded that the current staffing model "...seems to be working quite well," and that it was fulfilling CATSA's objectives at a reasonable cost.¹³⁵⁵ The Panel recommended, however, that the *CATSA Act* continue to permit all three delivery models for future consideration and flexibility. Transport Canada confirmed that the *CATSA Act* will retain all three delivery models as options.¹³⁵⁶ CATSA has since reviewed the three different service delivery models and decided to continue with the contract model.

The Auditor General of Canada produced a Special Examination Report in 2006 about CATSA's operations. The report noted some difficulties in the current recruitment model. For example, at least five major airports in Canada had to replace their contracted providers since 2004.¹³⁵⁷ One airport replaced screening providers four times, and another, three times. This makes the recruitment and retention of screening officers more difficult. Although a new screening contractor may hire many of the screening officers working for the previous contractor, the new contractor will also need to hire new screeners, adding to training costs. CATSA estimated the recent cost of contracted provider turnover at more than \$2.5 million.¹³⁵⁸ CATSA has recognized these problems and is beginning to improve its contracting process through measures such as placing greater weight on technical competence when selecting screening contractors.

Until recently, CATSA provided no guidance to screening contractors about hiring screening officers.¹³⁵⁹ Once hired, screening officers are required to read, understand and remain up-to-date on large amounts of detailed and continually updated security material, identify dangerous objects visually, and converse with passengers during screening. However, the Auditor General's report indicated that CATSA did not impose minimum education requirements for

¹³⁵² *CATSA Act*, ss. 6, 7.

¹³⁵³ Exhibit P-169, p. 104 of 202.

¹³⁵⁴ Exhibit P-169, p. 107 of 202.

¹³⁵⁵ Exhibit P-169, p. 107 of 202.

¹³⁵⁶ Exhibit P-101 CAF0871, p. 1.

¹³⁵⁷ Exhibit P-173, p. 50 of 64.

¹³⁵⁸ Exhibit P-173, p. 50 of 64.

¹³⁵⁹ Exhibit P-173, p. 34 of 64.

screeners.¹³⁶⁰ Under the *Designation Standards for Screening Officers*, discussed below in connection with training, applicants for screening officer positions must be at least 18 years old, Canadian citizens or permanent residents, able to effectively speak, read, and write one or both official languages, and certified as in good physical health. They must also meet minimum requirements for sight and hearing. The Standards also require applicants to hold a valid Transportation Security Clearance.¹³⁶¹

Particular difficulties arise in hiring and retaining enough bilingual screening officers in cities with only small French-speaking populations. CATSA does not require tests for proficiency in English or French.¹³⁶² Because of the lack of bilingual screeners, the Commissioner of Official Languages concluded both in 2004 and 2005 that CATSA failed to meet the requirements of the *Official Languages Act*. CATSA's contracts with screening contractors require them to ensure that the public can be served in both official languages. The Auditor General's report stated that CATSA must ensure that its subcontractors respect the language clauses in their contracts and provide bilingual services.¹³⁶³

The Auditor General's report recommended that CATSA provide greater guidance to its screening providers in hiring screening officers.¹³⁶⁴ CATSA management agreed with this recommendation, noting that the *Designation Standards for Screening Officers*, published by Transport Canada, prescribe the minimum qualifications for screening officers and the duties they must be able to perform. The *Canadian Aviation Security Regulations* require all screening officers to meet these standards.¹³⁶⁵

Another recruitment difficulty noted by the CATSA Advisory Panel related to the level of pay that might be required to attract the best applicants. It noted the case of Alberta, where the then-booming economy offered many job opportunities. Airport screening officers there were paid significantly less than other workers holding comparable jobs.¹³⁶⁶ This made it difficult to attract and retain highly qualified airport screeners. The Auditor General's report also noted the recruitment difficulties¹³⁶⁷ and that the lengthy wait by screeners for security clearances was contributing to a shortage of screeners throughout Canada. It might take several months for a newly hired screener to obtain a Transportation Security Clearance. Without this, prospective screening officers could not receive an RAIC card or undergo training.¹³⁶⁸ This made it even more difficult to hire screeners, since applicants might be unable or unwilling to wait for the clearance process to be completed, particularly in a bustling job market with many other opportunities.

¹³⁶⁰ Exhibit P-173, p. 34 of 64.

¹³⁶¹ Online: Canadian Air Transport Security Authority <<http://www.catsa-actsa.gc.ca/so-ac/english/legislation/designation.htm>> (accessed October 30, 2009).

¹³⁶² Exhibit P-173, p. 34 of 64.

¹³⁶³ Exhibit P-173, p. 35 of 64.

¹³⁶⁴ Exhibit P-173, p. 39 of 64.

¹³⁶⁵ *Canadian Security Aviations Regulations*, S.O.R./2000-111, ss. 6, 7.

¹³⁶⁶ Exhibit P-169, p. 120 of 202.

¹³⁶⁷ Exhibit P-173, p. 33 of 64.

¹³⁶⁸ Exhibit P-169, p. 130 of 202.

As of April 1, 2008, Transport Canada had completed a detailed audit of the security clearance process to determine the causes of delay in issuing clearances, as the CATSA Advisory Panel recommended. Transport Canada stated that it had begun to take steps to correct the deficiencies identified in the process and to speed it up.¹³⁶⁹

The CATSA Advisory Panel also found that many screening officers, especially at larger airports, held more than one job. At larger airports, 50 per cent of the screening work force had two, or even three, jobs.¹³⁷⁰ In areas where the cost of living was high, or where screening officers had significant family responsibilities, their income as screeners was insufficient. This forced them to take part-time or even other full-time work. These jobs were often at the same airport, such as at a retail outlet or an air carrier check-in counter. It was much more difficult to organize the work shifts for screening officers who had more than one job, increasing the risk that screening points would be understaffed.

CATSA manages staffing shortfalls in several ways, such as by paying overtime to screeners, particularly during peak periods.¹³⁷¹ Whether working overtime at a PBS or HBS screening point or working at multiple jobs, screening officers are much less likely to be alert and motivated if stressed or fatigued by long working hours.

CATSA also manages staff shortages by posting fewer screening officers on screening lines during peak periods. This means one officer performs two functions, such as both explosives trace detection and carry-on baggage searches.¹³⁷² CATSA has also responded to shortages by moving screeners from NPS to PBS. As a result, NPS is less effective and may diminish airport security. Finally, CATSA may deploy “Level 0” screeners – those who do not yet have a security clearance and training – to serve as “greeters” at the beginning of the screening line,¹³⁷³ after a basic background check by the police.¹³⁷⁴

CATSA has acknowledged the many concerns expressed about its hiring and retention problems and has sought to remedy these with changes to salaries, benefits, job descriptions and pre-selection testing, as well as changes to career planning and specialization. According to Pierre Cyr, CATSA’s Vice President of Strategic and Public Affairs, CATSA named one of its general managers as the coordinator responsible for hiring, training, retention, and security clearance. Cyr also testified that CATSA has developed and implemented a visual pre-test, in co-operation with the University of Zurich. Prospective screening officers would undergo this test to identify those unable to recognize certain images on a screen. About 25 per cent of the population has a visual deficiency that prevents easily recognizing certain images. Eliminating these individuals from

¹³⁶⁹ Exhibit P-101 CAF0871, p. 1.

¹³⁷⁰ Exhibit P-169, p. 120 of 202.

¹³⁷¹ Exhibit P-169, p. 120 of 202.

¹³⁷² Exhibit P-173, p. 33 of 64.

¹³⁷³ Exhibit P-173, p. 33 of 64.

¹³⁷⁴ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4806.

the pool of prospective screeners means that more applicants who have the necessary visual capabilities will complete selection and training programs.¹³⁷⁵

In response to the Auditor General's comments about staff shortages and high turnover, CATSA stated that the shortage of screening officers did not compromise security, but merely slowed passenger throughput at screening points.¹³⁷⁶ CATSA also indicated that screening officers were required to follow its Standard Operating Procedures (SOPs) to ensure that security is not compromised. However, given the stress, fatigue and potential for distraction or inattentiveness on the part of screening officers caused by staffing shortages, additional duties, and second jobs, the Commission questions CATSA's assurances.

The CATSA Advisory Panel expressed concern that credit checks were no longer being conducted in the security clearance process for screeners.¹³⁷⁷ Transport Canada had ended such checks. The Panel was concerned that, without credit checks to identify candidates with potential financial troubles, new screeners (and, for that matter, any airport employee) with significant money worries could pose a security risk. Indebted employees could engage in theft, already widespread at airports or, worse, accept bribes to commit or facilitate serious criminal activities at airports.

3.7.2 Training

The CATSA Act requires CATSA to set standards for the qualifications, training and performance of screening contractors and screening officers that are at least as stringent as those set by the aviation security regulations of the *Aeronautics Act*.¹³⁷⁸ CATSA relies on the *Designation Standards for Screening Officers* issued by Transport Canada for guidance.

Under the CATSA Act, both screening contractors and prospective screening officers must be certified as meeting CATSA's qualification, training and performance requirements.¹³⁷⁹ Screening officer applicants who have successfully completed their training are formally evaluated for their proficiency in each screening technique as well for other skills, such as resolving alarms, implementing emergency response procedures and exercising care and control over baggage. Depending on their proficiency, screening officer applicants receive endorsements for different skills, which are then itemized on a certificate indicating that they have been certified by CATSA as capable of properly conducting their duties and meeting performance standards. Screening officers must present their certificates when asked by a Transport Canada security officer. The prospective screening officers must also be designated in writing by

¹³⁷⁵ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4806.

¹³⁷⁶ Exhibit P-173, p. 39 of 64.

¹³⁷⁷ Testimony of Chern Heed and Jacques Bourgault, vol. 38, June 1, 2007, p. 4641.

¹³⁷⁸ CATSA Act, ss. 8(1), 8(2).

¹³⁷⁹ CATSA Act, s. 8(2).

the Minister of Transport before they can conduct searches authorized by the *Aeronautics Act*.¹³⁸⁰

CATSA recently implemented an in-house training program for contract screening officers. The CATSA National Training and Certification Program focuses on developing fundamentals such as familiarity with security technology and good interpersonal skills.¹³⁸¹ The program is based on regulatory requirements.¹³⁸² CATSA must certify the screening contractors or screening officers as satisfying these requirements before the contractor or screener can provide screening services. CATSA has the authority to vary, suspend or cancel the certification if a screening contractor or officer no longer satisfies the requirements. The program is also based on different proficiency levels for the screeners, ranging from that of basic screening officer to specialist, as well as supervisory and even instructor levels.

Screening officers are expected to know and comply with CATSA's SOPs, which it developed based on the requirements of the *Security Screening Order*.¹³⁸³ During training, CATSA's screening officers must become familiar with over 740 pages of such policies and procedures.¹³⁸⁴ The SOPs can be amended by CATSA Screening Operations Bulletins and can also be superseded by Transport Canada Security Notices. Screening officers must remain up-to-date with this material throughout their careers. This is facilitated by a new CATSA website. Besides training in security screening, screening officers receive training in courtesy and public relations to prepare them to interact with the public and to minimize conflicts.¹³⁸⁵

The Auditor General noted that CATSA's training program was under considerable stress due to employee turnover, the ever-growing need for screening officers at Canada's busy airports and the requirement to re-certify screening officers every two years. CATSA is responding by streamlining training content and by providing more intensive, higher-quality training, shortening the training time required through reductions in classroom time and on-the-job training. Additional training is being provided to screening officers doing HBS and NPS.¹³⁸⁶

The CATSA Advisory Panel raised a concern about the screeners' "Point Leaders."¹³⁸⁷ These are screening officers who have achieved a higher level of certification through extra CATSA training and, in some cases, through seniority. They are responsible for monitoring the operations of screening points and the work of the screening officers. Point Leaders may not receive significant training

¹³⁸⁰ *Aeronautics Act*, s. 4.84.

¹³⁸¹ Exhibit P-169, p. 120 of 202.

¹³⁸² Exhibit P-172, p. 62 of 155.

¹³⁸³ Exhibit P-169, p. 86 of 202.

¹³⁸⁴ Exhibit P-173, p. 35 of 64.

¹³⁸⁵ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4826.

¹³⁸⁶ Exhibit P-173, p. 35 of 64.

¹³⁸⁷ Exhibit P-169, p. 114 of 202.

in leadership and are frequently concerned with relatively trivial details such as monitoring break times. The Panel was concerned that there may be great variability in the activities of the Point Leaders and that CATSA managers did not provide sufficient oversight. Point Leader training is now being improved.¹³⁸⁸

An additional issue is whether the mandate of screening officers should expand to include searching passengers and baggage for large amounts of currency and illicit substances such as narcotics. Jim Marriott, Transport Canada's Director of Aviation Security Regulatory Review, testified that the proper training emphasis for screening officers is the prevention of unlawful interference with civil aviation. Cyr agreed, testifying about CATSA's perspective:

The more objects you ask a screener to try to identify the less focussed he is on weapons and improvised explosive devices that we absolutely don't want to be on board an aircraft.... I think it stands to reason that if we start asking them to look for a multitude of other objects, their attention will be moving to every direction and the risk of missing an item that could create a threat to air transportation security would be greater.

...

And of course, if we happen to find – what you call contraband, whether it's large sums of money – which sometimes appear as a mass which needs to be identified, then we call the police. Sometimes we find drugs by accident, also by doing pat-downs, the police [are] called, and the passenger and the object is given to the police but this is not our main reason, our main reason is to protect the air transportation system.¹³⁸⁹

Dr. Kathleen Sweet, a US-based aviation security expert, agreed that a more diffuse focus for screeners was inappropriate: "...[W]hen you have [screeners] looking for marijuana or looking for cocaine, they're not looking for a bomb."¹³⁹⁰ She testified that, at some airports, screeners receive a cash incentive when they find and report narcotics and that this only distracts them from their primary responsibility to ensure air safety. For similar reasons, the CATSA Advisory Panel opposed training and requiring screeners to search for narcotics or other illicit substances.¹³⁹¹

CATSA implemented two training programs to provide screening officers with hands-on experience in identifying objects that may pose a threat. The programs

¹³⁸⁸ Exhibit P-173, p. 35 of 64.

¹³⁸⁹ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4802-4803.

¹³⁹⁰ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4969-4970.

¹³⁹¹ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, pp. 4644-4645; Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4645.

have been deployed at all Class 1 and 2 airports in Canada. These programs are important because screening officers only rarely encounter weapons and other dangerous objects, yet they must be able to identify them.¹³⁹²

The first system, known as the X-ray Tutor (XRT),¹³⁹³ is an X-ray simulation that allows screening officers to practise operating an X-ray machine in a discrete training area under controlled conditions. As the officer becomes proficient at identifying the dangerous items displayed within the images of bags on the X-ray display, the simulation program becomes progressively more challenging. The dangerous items become harder to find and identify. After completing their training, CATSA screening officers are required to spend 20 minutes each week with the XRT to refresh their skills.¹³⁹⁴ Nick Cartwright, Director of the Security Technology Branch, Security and Emergency Preparedness at Transport Canada, testified that the XRT system tracks the screening officer's progress and can target weaker areas to help improve their performance.

The Auditor General's report stated that, while CATSA deployed XRT systems across the country, there were problems with the program. There were not always enough computers equipped with XRT for screening officers, and some computers were not in convenient locations.¹³⁹⁵ In addition, the initial reports of XRT usage compiled by CATSA showed that screeners were not using XRT in large numbers, and that many who did were not progressing to the higher and more difficult levels. CATSA management acknowledged these difficulties, and CATSA is looking into more extensive use of XRT.

A second program, the Threat Image Projection System (TIPS), is used at screening points in airports. TIPS is a computer system that superimposes images of a weapon or explosive device on the display screen of an X-ray machine while a bag is being scanned. The fictitious dangerous item appears to be within the bag itself. Threat image projection is primarily used in PBS but it is beginning to be used at other screening points, such as HBS.¹³⁹⁶ Both TIPS and the XRT provide training, and the TIPS program has the added advantage of helping to motivate screening officers. When a screening officer identifies a dangerous item on the X-ray screen, the officer must respond accordingly, and the device acknowledges their performance with a message. Transport Canada was reluctant, for security reasons, to indicate the general success rate of screening officers who use TIPS or the degree to which its use has improved their abilities. However, Cartwright testified that academic studies have confirmed that the use of TIPS significantly enhances the motivation of the screening officers and provides them with ongoing experience in identifying dangerous items.¹³⁹⁷

¹³⁹² Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5089.

¹³⁹³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5096.

¹³⁹⁴ Exhibit P-173, pp. 35-36 of 64.

¹³⁹⁵ Exhibit P-173, p. 36 of 64.

¹³⁹⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5088-5090.

¹³⁹⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5089.

Screening officers must be re-certified every two years. CATSA provides informal training through online seminars that explain new procedures, which are set out in screening bulletins to CATSA Point Leaders, and runs “training bags” containing simulated prohibited items through screening points.¹³⁹⁸ On average, 20 new screening bulletins are issued each year as procedures and threats to aviation security change. CATSA also provides a bulletin board at each airport that depicts different types of improvised explosive devices (IEDs), to acquaint screening officers with the appearance and design of such devices. However, feedback from screening officers indicates that this has not done enough to familiarize them with IEDs. The Commission heard evidence that explosive devices had been found concealed in stuffed animals and even sex toys, objects that would not necessarily receive a great deal of scrutiny.¹³⁹⁹ Only confident, well-trained and diligent screening officers would examine such objects in the necessary detail.

The CATSA Advisory Panel recommended that CATSA do more ongoing training and refresher training for all screening personnel, particularly about new techniques to detect IEDs.¹⁴⁰⁰ Similarly, the Auditor General’s report expressed concern about the limited formal refresher training provided to screening officers, pointing out that, in 2004, screening officers received a one-day training course. The Auditor General called for CATSA to ensure that screening officers were properly trained and individually equipped to adapt to the constantly changing working environment.¹⁴⁰¹ The Auditor General also recommended that CATSA refresher training include more than X-ray recognition, and that it cover topics such as changes to the CATSA SOPs. The report stated that training should also emphasize practical skills, like the proper use of the hand-held metal detector and other passenger and baggage search techniques.¹⁴⁰² Finally, the training bags used at checkpoints should be changed periodically to include new and different threat objects.

Sweet testified about the importance of ongoing retraining and of fostering a culture of security awareness among everyone working at airports, not merely the screeners:

The key here is doing proper training in the first place and then keeping the training constant. You don’t train somebody and then two years later, train them again. And if somebody makes a mistake on the line, you retrain them then, and you don’t just retrain them on one set of software, because they get used to picking out the bag that’s in the software exam.

¹³⁹⁸ Exhibit P-173, p. 36 of 64.

¹³⁹⁹ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4698.

¹⁴⁰⁰ Exhibit P-169, p. 121 of 202.

¹⁴⁰¹ Exhibit P-173, pp. 35-36 of 64.

¹⁴⁰² Exhibit P-173, p. 36 of 64.

You know, we don't do the training of these screeners very well and we don't give them a positive enough attitude about their job. That's why I'm a proponent of – I meant to underline the word "all." All people – anybody who works at the airport should have some type of security awareness training, whether it's the janitor or whether it's the pilot or whether it's the airport manager.¹⁴⁰³

Most important, the Auditor General's report urged CATSA to ensure adequate training resources. The report noted how thinly stretched CATSA Learning and Performance Advisors were. Eight full-time and nine contract instructors conducted the screening officer training and recertification programs.¹⁴⁰⁴ The instructors might be required to teach two full-day courses each day, working from 7:00 a.m. until 11:00 p.m., and often had to travel considerable distances between airports. Many screening officers had their mandatory recertification testing rescheduled because of a lack of available training staff.

3.7.3 Turnover

The high turnover rate among screening officers creates many problems. Staffing shortages result in long working hours for screening officers, and having to perform multiple duties increases fatigue and decreases alertness and motivation. The cost of training a screening officer is significant – about \$4000, besides other costs such as those for new uniforms.¹⁴⁰⁵ Each new employee must also undergo a lengthy security clearance process, causing further delays and strains to the screening system. It is essential to reduce the turnover rate for both security and cost reasons.

Several factors contribute to the relatively high turnover of screening officers, including lengthy delays in obtaining security clearances, low rates of pay, highly competitive job markets and the perceived lack of advancement opportunities and prestige. The CATSA Advisory Panel suggested that the nature of the job – monotonous, stressful work requiring constant vigilance – contributed significantly to the turnover. According to the Panel, the average turnover rate at Canada's eight Class 1 airports in 2005–2006 was a "respectable" 12.2 per cent. However, the Auditor General's report noted that in the final quarter of 2006, the turnover rate increased to 16.4 per cent.¹⁴⁰⁶ The turnover rate varies greatly from region to region, depending on competing employment opportunities.¹⁴⁰⁷ For example, Toronto and Vancouver International Airports had low annual turnover rates of 6.5 and 3.8 per cent respectively. At four other Canadian international airports (including Calgary, Edmonton and Winnipeg), the rate ranged between 26.4 per cent and 34.6 per cent.¹⁴⁰⁸

¹⁴⁰³ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4952–4953.

¹⁴⁰⁴ Exhibit P-173, pp. 36–37 of 64.

¹⁴⁰⁵ Exhibit P-169, p. 119 of 202.

¹⁴⁰⁶ Exhibit P-173, p. 10 of 64.

¹⁴⁰⁷ Exhibit P-169, p. 105 of 202.

¹⁴⁰⁸ Exhibit P-173, p. 33 of 64.

The average annual turnover of screening personnel at the 19 largest airports in the US was 126 per cent per year in 1998-99. It has declined significantly to about 20 per cent annually since then. Screeners at US airports are now employees of the Transportation Security Administration (TSA), not employees of private companies. The still high rate of turnover can be explained in part because the TSA screening officer position is seen as a possible entry point into the federal civil service.¹⁴⁰⁹

CATSA is aware that high employee turnover is costly, inefficient and demoralizing for an organization. It has worked to attract and retain the highly skilled, highly motivated personnel needed for this stressful work by negotiating a significant pay increase. One of its first initiatives was to negotiate pay increases of about 50 per cent, resulting in an average wage of \$15 an hour in 2006. This was considered generally competitive in most areas of the country.¹⁴¹⁰ Cyr testified that CATSA instituted a supplementary income program at some Alberta airports to attract and retain screeners in the highly competitive job market there.¹⁴¹¹ At the airport where the program was first tried, the attrition rate dropped by 68 per cent. The program was then extended to the Calgary and Edmonton airports. Those promoting the program hoped it to be self-financing because of the large savings realized by having to train far fewer new workers. CATSA also updated its Performance Payment Program to boost retention. The program is in essence a bonus paid to contracted screening provider companies. CATSA tied a significant part of the bonus funds to the retention of screening officers. This created a strong incentive for screening providers to select and retain high quality employees.¹⁴¹²

CATSA also rotates screening officers from duty to duty on a regular basis to ensure that they remain alert and do not become distracted or bored. In addition, screeners are permitted to work at X-ray machines for only 15 minutes at a time to prevent boredom and fatigue.¹⁴¹³

Sweet recommended regular low-level security briefing to provide screeners with a greater sense of mission.¹⁴¹⁴ She discussed a pilot project at Dulles International Airport, near Washington DC, where screeners regularly received intelligence briefings from the FBI and other intelligence agencies. The screening officers did not receive highly classified information, only security information pertinent for that airport for that day. Sweet testified that such briefings enhanced the screeners' diligence, security awareness, and motivation. Cyr testified that, in Canada, it would be extremely unlikely that CSIS or other intelligence officials would be willing and able to brief all CATSA screening officers at 89 airports each day. He stated that screening officers receive information from CATSA and Transport Canada through bulletins and briefings by their Point Leaders.¹⁴¹⁵

¹⁴⁰⁹ Exhibit P-169, p. 105 of 202.

¹⁴¹⁰ Exhibit P-169, p. 119 of 202.

¹⁴¹¹ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4806.

¹⁴¹² Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4806-4807.

¹⁴¹³ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4809.

¹⁴¹⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4968-4969.

¹⁴¹⁵ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4810.

The Auditor General and the CATSA Advisory Panel have both acknowledged the importance of providing accessible, timely information through retraining and other regular updates. The Commission also believes that serious consideration should be given to providing briefings, at selected Class I airports, of the type suggested by Sweet.

3.7.4 Testing

Transport Canada tests whether dangerous items are being detected and prevented from entering the restricted areas of an airport. These infiltration tests are an important way to gauge the effectiveness of security measures. Testing screening points helps identify both human failure and deficiencies with screening equipment and procedures. Such testing is pointless, however, without proper feedback and follow-up. Plans to correct deficiencies must be developed and diligently carried out. This also requires adequate sharing of information between Transport Canada and CATSA, and within CATSA itself.

Transport Canada security inspectors conduct infiltration tests by attempting to bring a concealed, dangerous item such as a knife or inoperative firearm or explosive device through a PBS checkpoint.¹⁴¹⁶ The inspectors note whether the screening officers successfully detect the unauthorized objects.¹⁴¹⁷ If they fail to detect the objects, Transport Canada sends an “enforcement letter” to CATSA, and CATSA managers are expected to provide a written response explaining how the failure is being addressed. The security inspectors also determine whether screening officers hold proper qualifications, and test whether unauthorized access to secure areas is prevented. The sole statistic tracked to measure the performance of airport security, however, is the “infiltration failure rate” – the rate at which screening officers fail to detect a threat object. The failure rate is classified information.

When CATSA receives an enforcement letter, it proposes remedies to Transport Canada. A range of remedies may be involved. Generally, screening officers who fail an infiltration test receive additional training. Service providers sometimes penalize screening officers who fail the infiltration test.¹⁴¹⁸

The Commission was given an example of a hypothetical screening officer who failed to interpret X-ray images properly during searches of baggage at a security checkpoint.¹⁴¹⁹ One option would be to decertify the individual for all or some of the individuals’ current screening certifications, such as that for X-ray screening. The individual would require retraining. Recurring violations might lead CATSA to terminate the individual’s employment.

Transport Canada security inspectors who observe poor screening performance have the authority to “de-designate” a screening officer by revoking, suspending

¹⁴¹⁶ Exhibit P-173, p. 20 of 64.

¹⁴¹⁷ Exhibit P-411, p. 17 of 48.

¹⁴¹⁸ Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4818.

¹⁴¹⁹ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4839-4840.

or cancelling the officer's certification.¹⁴²⁰ Certification means that the screening officer is trained and proficient at their duties, and designation means that the individual is a legal authority with certain search powers that flow from the *Aeronautics Act*. The individual cannot work as a screening officer until the designation and CATSA certification are reinstated. De-designated screening officers have a right of appeal to the Transportation Appeal Tribunal of Canada, a quasi-judicial body.

Sweet testified that being removed for retraining was generally the best remedy for screeners who failed an infiltration test or who performed poorly on the TIPS system. She pointed to the example of Athens airport, where a strict policy is applied to remove from the line any screeners who miss a TIPS image and to provide them with further training at an on-site facility. She testified that if the screeners were not removed and retrained, they would repeat the mistake.¹⁴²¹

The evidence before the Commission did not clearly demonstrate a need to disclose the failure rates of infiltration tests. However, there must be continual pressure placed on all those involved in aviation security to ensure that identified weaknesses are quickly corrected in order to maximize security and justify the public's investment in CATSA and its confidence in Canada's aviation security regime as a whole.

There was little support within the aviation security community for publishing infiltration test failure rates.¹⁴²² Instead, the experts who testified at the Commission placed greater importance on ensuring that deficiencies are identified and corrected. They stressed that testing alone is not enough; it is vital to follow with solutions and to make sure that they are properly implemented.

In contrast, the Senate Standing Committee on National Security and Defence recommended publishing a summary of intrusion test results after some reasonable period of delay during which the deficiencies could be remedied.¹⁴²³ The Committee had obtained information from "senior officials" that led its members to conclude that the failure rate was unacceptably high. The Committee suggested that disclosing such information would allow the public to decide for itself whether air travel was sufficiently safe, and would place additional pressure on CATSA and screening providers to strive for better results. Disclosure of intrusion test results is discussed in greater detail in Section 3. 9.¹⁴²⁴

TIPS and XRT provide additional means to assess the skills of screening officers in detecting dangerous objects. The CATSA Advisory Panel encouraged continuing with TIPS and XRT to provide practice, rate performance and give direct feedback to screening officers. Significantly, the Panel recommended

¹⁴²⁰ Exhibit P-169, p. 87 of 202.

¹⁴²¹ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4966-4971.

¹⁴²² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5050; Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5284.

¹⁴²³ Exhibit P-172, p. 81 of 155.

¹⁴²⁴ Duty to Warn and Transparency in Aviation Security.

against using results as the basis for punitive actions such as fines, penalties, reprimands or decertification. The focus instead should be on continuous learning and improving performance. The Panel also reported that screening officers had a favourable view of using such tools for instruction and feedback. It noted, however, that budget limitations prevented deploying these systems widely enough to make TIPS and XRT accessible and practical for all screening officers.¹⁴²⁵

CATSA uses closed-circuit television (CCTV) at all screening checkpoints. However, CATSA opposes the use of CCTV to monitor screening officer performance, since its employees strongly object to such intrusive observation. CATSA management also made the business decision not to use CCTV for this purpose due to the complexity and expense of such a measure, and because it believed that other, more effective, ways existed to monitor and evaluate screening officers. These included hiring compliance monitors at airports and better training for CATSA Point Leaders.¹⁴²⁶

If an incident occurs at a checkpoint, such as a security breach or a report of a missing item, any passengers or objects involved can be identified from the CCTV images recorded at the checkpoint. CATSA Headquarters can monitor all its screening lines across Canada in this manner. All 200 checkpoint CCTV cameras are monitored on a rotating basis from 6:00 a.m. until 10:00 p.m. daily. Recordings are kept for 15 days. However, if a security event occurs, the recordings can be stored for future reference.¹⁴²⁷

In a 2005 report on national security, the Auditor General identified flaws in the security inspection and enforcement. Neither CATSA nor Transport Canada possessed an accurate and complete inventory of the enforcement letters that had been sent or of CATSA's written responses.¹⁴²⁸ The Auditor General could find no response to about 12 per cent of the enforcement letters about infiltration tests, and about 16 per cent of the enforcement letters about other security deficiencies. Although CATSA then changed its procedures to track both enforcement letters and responses more carefully, a 2006 report of the Auditor General noted that, in most cases, CATSA management still did not provide written responses to either CATSA Headquarters or to Transport Canada, and found that CATSA's performance in this area had actually worsened since the 2005 report.¹⁴²⁹

Following publication of the Auditor General's 2006 report, CATSA took steps to ensure that every corrective action taken at airports regarding infiltration test failures was documented, both at the airport and at CATSA Headquarters. In addition, CATSA now reconciles its records with Transport Canada monthly to verify that all failed infiltration tests have been reported.¹⁴³⁰

¹⁴²⁵ Exhibit P-169, p. 121 of 202.

¹⁴²⁶ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4833-4835.

¹⁴²⁷ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4816-4817.

¹⁴²⁸ Exhibit P-411, p. 17 of 48.

¹⁴²⁹ Exhibit P-173, p. 38 of 64.

¹⁴³⁰ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4817-4818.

Both CATSA management and Transport Canada inspectors expressed frustration with each other over infiltration tests.¹⁴³¹ The inspectors pointed out to the CATSA Advisory Panel that, on many occasions, CATSA did not appear to provide timely replies to letters of contravention issued by the inspectors. The inspectors also took the view that changes needed to remedy infractions were not always implemented. Some inspectors informed CATSA that they believed screening officers were being recertified without proper retraining and testing after a negative inspection report. Conversely, CATSA expressed concerns to the Panel about the inflexible application of highly prescriptive rules governing CATSA's screening operations.

Other times, Transport Canada and CATSA disagreed about the meaning and application of the detailed regulations, orders, measures and SOPs that prescribe CATSA's screening operations. The CATSA Advisory Panel noted confusion about whether inspectors are to gauge screening officer performance based on CATSA SOPs or on Transport Canada's *Security Screening Order*.¹⁴³² There were disagreements even as to the meaning of "random selection" at screening points. Such confusion could contribute to the anxiety of screening officers as they carried out their duties. Because of these disputes, the Panel recommended the application of clear, consistent, mutually understood standards for monitoring screening officers. The Commission agrees with the Panel. According to the most recent information available, Transport Canada is still considering the Panel's recommendation.¹⁴³³

The Auditor General's 2005 report also noted flaws in the oversight and enforcement model.¹⁴³⁴ In particular, Transport Canada had not defined any system-wide performance standards for CATSA, apart from the infiltration failure rate, by which its compliance and effectiveness could be assessed. In addition, CATSA did not face monetary penalties, unlike air carriers or airport authorities, which would be fined for persistent non-compliance with security requirements. According to the report, Transport Canada decided not to introduce monetary penalties for CATSA because fines would redirect resources from the implementation of CATSA's security mandate.

The CATSA Advisory Panel acknowledged that it might not be appropriate to exact monetary penalties from a Crown corporation funded by the public, but questioned whether the oversight model could provide for effective enforcement actions against CATSA.¹⁴³⁵ The Auditor General recommended that Transport Canada develop performance measures for CATSA that specify what constitutes satisfactory performance.¹⁴³⁶ The CATSA Advisory Panel endorsed this recommendation.¹⁴³⁷

¹⁴³¹ Exhibit P-169, p. 140 of 202.

¹⁴³² Exhibit P-169, p. 88 of 202.

¹⁴³³ Exhibit P-101 CAF0871, p. 2.

¹⁴³⁴ Exhibit P-411, pp. 17-18 of 48.

¹⁴³⁵ Exhibit P-169, p. 88 of 202.

¹⁴³⁶ Exhibit P-411, p. 18 of 48.

¹⁴³⁷ Exhibit P-169, pp. 88-89 of 202.

The CATSA Advisory Panel also concluded that Transport Canada's de-designation power was unnecessary and that, since CATSA is responsible for training screening officers, it should have the sole responsibility for "sanctioning" them.¹⁴³⁸ Rodney Wallis, former Director of Security at the International Air Transport Association (IATA), testified that it was important to keep the oversight structure simple. If a Transport Canada inspection identified problems with a screening officer's performance, the obvious recourse would be to inform CATSA management.¹⁴³⁹ CATSA would then be responsible for responding to the inspection findings, and Transport Canada would be charged with monitoring the response.

Jean Barrette, Transport Canada's Director of Security Operations, explained that the Department was still considering the Panel's recommendation. He stated that the decision as to whether the de-designation power should be delegated to CATSA involved many complicated issues. The certification and designation of screening officers were two separate and necessary qualifications. Barrette testified that Transport Canada retained the designation authority after CATSA was created to enable the Department to exercise objective and independent oversight over CATSA as a legislated entity. In addition, if CATSA were given the designation and de-designation power, it would have additional responsibilities. One would be to represent the Minister of Transport at the Transportation Appeal Tribunal of Canada, the consequences of which Transport Canada wished to consider carefully. Transport Canada was reluctant to give up its oversight role before fully contemplating the implications.¹⁴⁴⁰

CATSA is authorized to conduct simulated intrusion tests as a component of screening officer training. These tests are conducted under controlled conditions away from restricted areas rather than while screeners are performing their duties. The results are used to measure performance and provide feedback to the screeners. The CATSA Advisory Panel considered this to be an effective and useful training tool.¹⁴⁴¹ Both the Auditor General and the Panel noted CATSA's dissatisfaction with the limited authority it had to conduct infiltration tests, and that CATSA management felt it needed to be able to conduct full infiltration tests, which would include the authority to take prohibited items through a screening checkpoint.¹⁴⁴²

There was considerable disagreement between CATSA and Transport Canada about the threshold for failing an infiltration test.¹⁴⁴³ Matters in dispute included which screening officer was responsible for identifying the threat object, and whether the screening officer correctly followed CATSA procedures in carrying out the failed screening. Such disputes damaged the relationship between Transport Canada and CATSA, and the Auditor General urged a speedy resolution of these issues in her 2006 report.¹⁴⁴⁴

¹⁴³⁸ Exhibit P-169, p. 87 of 202.

¹⁴³⁹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5042-5043.

¹⁴⁴⁰ Testimony of Jean Barrette, vol. 39, June 4, 2007, pp. 4836-4841.

¹⁴⁴¹ Exhibit P-169, p. 121 of 202.

¹⁴⁴² Exhibit P-173, p. 20 of 64; Exhibit P-169, p. 149 of 202.

¹⁴⁴³ Exhibit P-173, p. 20 of 64.

¹⁴⁴⁴ Exhibit P-173, p. 21 of 64.

3.7.5 Conclusion

There are many indications that CATSA and Transport Canada have recognized the difficulties associated with recruiting, training, retaining and testing screening officers, and that the two bodies have done considerable work to overcome those difficulties. Ensuring that screening officers are well-trained, attentive and skilled is essential for aviation security. It is also essential to hire the candidates with the best potential to become effective and motivated screening officers.

As with aviation security in general, however, there is no room for complacency about the improvements needed. Airports in 1985 had strikingly inadequate security, due in large part to the complacency, poor training and poor discipline of the private security guards hired to screen passengers and baggage. A failure by other airport employees to adopt a vigilant and informed attitude towards security compounded this inadequacy. Security at Canadian airports is improved today, but the human dimension of aviation security remains a concern. As long as human judgment and skill remain integral components of airport security, every effort must be made to ensure that training and re-training is of the highest quality and readily available, and that performance standards are clear and consistent. Only in this way can the competence, motivation, and vigilance of the individuals involved in carrying out aviation security measures be improved.

3.8 Closing the Gaps in Aviation Security

3.8.1 Air Cargo

The next act of sabotage against civil aviation could well target air cargo. Carried primarily on passenger aircraft,¹⁴⁴⁵ air cargo in this country is not routinely searched before it is loaded,¹⁴⁴⁶ and the screening measures applied to those who present air cargo for transport are insufficient.¹⁴⁴⁷ In many respects, the state of air cargo security today is disturbingly similar to that of the security applied to checked baggage before the loss of Air India Flight 182. At the time, the few security controls that applied to baggage were insufficient to meet the known threat of sabotage. Security measures were available that could have prevented placement of the suitcase containing the bomb on the flight, but were simply not implemented.

The security regime of the day suffered from poor regulatory oversight, a lack of vigilance, a culture of complacency, excessive concern for customer convenience and a reactive approach to security threats. The bombing of Flight 182 showed the devastating consequences of sabotage directed against civil aviation. While baggage security has largely overcome the failings that made the Air India bombing possible, the same cannot be said for the security of air cargo.

¹⁴⁴⁵ Testimony of Craig Hall, vol. 64, October 24, 2007, p. 8008; see also Exhibit P-169, p. 53 of 202.

¹⁴⁴⁶ Exhibit P-169, p. 52 of 202.

¹⁴⁴⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4630.

Air cargo, conveyed in the same hold of passenger aircraft as checked baggage, shares many characteristics with baggage. Cargo and baggage are both generally prepared for transport before they are taken to the airport and both can conceal explosives. In some instances, baggage is expressly conveyed as air cargo.¹⁴⁴⁸ In fact, representatives of Air India contended at the hearings that the "M. Singh" suitcase that was permitted to be placed on Flight 182 was properly characterized as air cargo rather than as unaccompanied interlined baggage.¹⁴⁴⁹ This argument is unpersuasive, however, since the suitcase was presented at the Canadian Pacific (CP) Air ticket counter as checked passenger baggage and was then labelled with an interline tag.¹⁴⁵⁰ Nevertheless, the similarities between air cargo and passenger baggage are unmistakeable.

As early as 1980, Transport Canada recognized air cargo, including mail, as a means for placing explosive devices on aircraft.¹⁴⁵¹ One of the world's first in-flight bombings of a passenger aircraft took place in Canada through an explosive device concealed in air cargo. On September 9, 1949, a bomb in a mailed package, and not in a passenger's baggage, destroyed a Canadian Pacific Airlines DC-3 while it was in flight near St. Joachim, Quebec, killing 19 passengers and 4 crew members. Three people were subsequently executed for the crime.¹⁴⁵² Security measures have nonetheless focused on passengers and their baggage. As a result, the threat to aircraft posed by bombs has been only partially addressed.

Initiatives to respond to the threat of sabotage developed slowly, with effective measures emerging mostly in reaction to particular events. In the aftermath of the Air India bombings, significant improvements were made to aviation security to address the threat posed by bombs. Since the late 1970s, explosives have displaced hijackings as the predominant threat. Passenger-baggage reconciliation has been the main security improvement.¹⁴⁵³ This mitigated the threat posed by unaccompanied baggage, but only addressed part of the security problem. Following the events of September 11, 2001, renewed

¹⁴⁴⁸ The Commission heard from several aviation security experts that there are circumstances in which unaccompanied baggage is clearly considered cargo. Rodney Wallis, for example, explained that baggage that is intentionally shipped separately by travelling passengers who wish to avoid excess baggage charges is cargo. Chern Heed, a former Airport General Manager for Vancouver International Airport and Toronto Lester B. Pearson International Airport, agreed with this categorization. See Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4408. See also Testimony of Chern Heed, vol. 37, May 31, 2007, p. 4378.

¹⁴⁴⁹ See, for example, Testimony of Rajesh Chopra, vol. 37, May 31, 2007, p. 4437.

¹⁴⁵⁰ Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the hearings, explained that the characterization of baggage is dependent on its associated control document. Thus, baggage can be deemed accompanied, unaccompanied, expedite or cargo based on its corresponding tag or other documentation. See Testimony of Jim Marriott, vol. 38, June 1, 2007, p. 4561.

¹⁴⁵¹ Exhibit P-101 CAF0163, p. 5.

¹⁴⁵² See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁴⁵³ Exhibit P-411, pp. 8-9. See also Wallis, *Combating Air Terrorism*, p. 77 and Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4942.

efforts were made to improve security, again aimed primarily at passengers and baggage, leaving critical gaps in air cargo security virtually untouched.¹⁴⁵⁴

The differences in security measures now applied to passengers and their baggage, on one hand, and air cargo, on the other, are striking. Passengers may board an aircraft only after a gauntlet of security screening tests: identification and boarding passes are verified, possibly several times, at checkpoints; names are checked against those on a "Specified Persons List" (sometimes colloquially called a "no-fly" list);¹⁴⁵⁵ a walk-through metal detector scans for prohibited items; and there may be a further examination by a hand-held metal detector or physical search.¹⁴⁵⁶ A secondary search may be performed at the boarding gate. Carry-on items are also heavily scrutinized through mandatory X-ray scanning, with a possible subsequent search by hand or by explosives-detecting trace (EDT) equipment.¹⁴⁵⁷ Thorough screening is also conducted to identify liquids and gels above a certain volume.¹⁴⁵⁸ Since January 1, 2006, every piece of hold baggage is screened by EDT equipment,¹⁴⁵⁹ and may pass through up to five levels of in-line equipment and review by screening officers.¹⁴⁶⁰ In contrast, air cargo, for the most part, is simply placed alongside baggage in the aircraft hold as long as the shipper has met the minimal criteria of having had a regular business relationship with the air carrier.¹⁴⁶¹ The image of fully screened passengers seated on aircraft with largely unscreened air cargo beneath them is troubling.

The value of improvements to passenger and baggage screening is greatly diminished if a bomb can be placed in a cargo shipment. This was the most disturbing revelation about Canada's current civil aviation security regime. It was also the one uniting factor among all the experts and stakeholders who appeared at the hearings. With striking unanimity, they agreed that air cargo currently represented one of the most significant gaps in aviation security, and that the gap must be addressed.¹⁴⁶² As the Standing Senate Committee on National Security and Defence (Senate Committee) observed in its 2003 report on aviation security, it appears that the "front door" of air security is fairly well secured, while the "side" and "back doors" remain wide open.¹⁴⁶³

The vulnerability of air cargo to exploitation for terrorist ends is even more troubling because the vast majority of air cargo in Canada – almost 80 per

¹⁴⁵⁴ Exhibit P-35, pp. 20-21; see also Exhibit P-411, p. 9.

¹⁴⁵⁵ Exhibit P-182, p. 4 of 5; see also Testimony of Brion Brandt, vol. 40, June 5, 2007, pp. 4862-4863.

¹⁴⁵⁶ Exhibit P-169, p. 64 of 202.

¹⁴⁵⁷ Exhibit P-169, p. 64 of 202.

¹⁴⁵⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5138.

¹⁴⁵⁹ Exhibit P-169, p. 65 of 202.

¹⁴⁶⁰ Exhibit P-169, p. 66 of 202.

¹⁴⁶¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5293.

¹⁴⁶² See, for example, Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003; see also Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4629, Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4246, Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4958-4959; Exhibit P-169, p. 52 of 202; Exhibit P-172, p. 40 of 155.

¹⁴⁶³ Exhibit P-171, p. 9.

cent – is carried on passenger aircraft.¹⁴⁶⁴ About one million tonnes of cargo is transported annually by air.¹⁴⁶⁵ The amount carried on passenger aircraft is therefore substantial. The air cargo industry represents a significant portion of Canada's economy, comprising 6.2 per cent of trade with the United States and 21 per cent of trade with other countries.¹⁴⁶⁶ With the amount of air cargo on passenger aircraft expected to double in the next two decades due to increasing trade with Asia, the security risk posed by air cargo will worsen if not adequately addressed.¹⁴⁶⁷

In the United States, only about 25 per cent of air cargo is carried on passenger aircraft. The US industry has economies of scale that permit most air cargo to be transported by all-cargo aircraft.¹⁴⁶⁸ Still, the security risk posed by air cargo on passenger aircraft in the US is significant, since there is air cargo on many passenger flights – about 6 billion pounds of cargo each year.¹⁴⁶⁹ As in Canada, aviation security in the US has been criticized for its focus on passenger and baggage screening to the relative exclusion of air cargo security. In 2005, the US Department of Homeland Security (DHS) reported that most air cargo on passenger aircraft was not physically inspected. That same year, legislation was enacted requiring additional steps to secure air cargo, including an increase in the percentage of cargo destined for passenger aircraft that was inspected.¹⁴⁷⁰

Despite their potential to do so, explosives hidden in air cargo on passenger aircraft have not caused a major aviation tragedy in decades.¹⁴⁷¹ This may explain the relative neglect of air cargo security over such an extended period. Rodney Wallis, former Director of Security at the International Air Transport Association (IATA) and an international civil aviation security consultant, was the Commission's primary expert in this area. He testified that air cargo has long been known to be susceptible to sabotage, but that aviation security measures are rarely formulated proactively. He stated that "the great leaps in aviation security activity" inevitably followed a major incident.¹⁴⁷² In 1993, he voiced this concern about air cargo:

History has shown that motivation to achieve good security frequently, perhaps normally, comes in the wake of tragic accidents like the loss of the Air India 747 in summer 1985. To date, cargo has caused little problem."¹⁴⁷³

¹⁴⁶⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4629; see also Exhibit P-169, p. 53 of 202.

¹⁴⁶⁵ Testimony of Chern Heed, vol. 38, June 1, 2007, pp. 4650-4651.

¹⁴⁶⁶ Exhibit P-169, p. 52 of 202.

¹⁴⁶⁷ Exhibit P-169, pp. 52-53 of 202.

¹⁴⁶⁸ Exhibit P-101 CAF0872, p. 3. In 2004, it was estimated that 23 billion pounds of cargo was shipped with the United States by air. About 75 per cent, or 17 billion pounds, travelled aboard all-cargo aircraft, while the remaining 6 billion pounds travelled aboard passenger aircraft. See Exhibit P-417, p. 12.

¹⁴⁶⁹ Exhibit P-417, p. 12.

¹⁴⁷⁰ Exhibit P-417, pp. 1-2.

¹⁴⁷¹ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁴⁷² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5010.

¹⁴⁷³ Wallis, *Combating Air Terrorism*, p. 79.

Even when a threat is known, it is often not perceived to be immediate. If competing interests are vying for the same limited resources, political commitment can falter. A 2005 report of the Auditor General of Canada, the second in a two-part review of the 2001 national Anti-Terrorism Initiative,¹⁴⁷⁴ observed that aviation security inspection resources were weighted towards passengers and baggage. The report found that risks from air cargo had attracted less scrutiny, notwithstanding the level of concern it had generated.

Passengers and baggage are now well-scrutinized by multiple layers of security controls. As a result, terrorists will naturally seek weaker links in the security chain. In 1993, Wallis observed:

As airline security programs make it more and more difficult to use passengers and their baggage to cover acts of sabotage, terrorists are bound to search for other avenues. Airlines must not overlook the possibility of cargo, including shipments of mail, becoming the chosen means.¹⁴⁷⁵

Dr. William Leiss, an expert in risk management retained by the Commission, maintained that proper risk management requires protecting all domains of risk to an acceptable level. Gaps in security weaken the entire system and increase risk. If such gaps exist, resources must be redistributed so that all risks are sufficiently addressed.¹⁴⁷⁶

Despite knowledge within the aviation community and government of the vulnerability of air cargo, air cargo security has changed little over nearly three decades. Only recently has the Government of Canada taken steps to improve it. A pilot project is now under way. This is long overdue.

3.8.1.1 Air Cargo Security: A Decades-old Concern

By 1980 the Government of Canada was aware of the vulnerability of air cargo to sabotage. In February of that year, the Joint Study Committee on Civil Aviation Security met to conduct an intelligence review. The Committee consisted of senior representatives of Transport Canada, the Air Transport Association of Canada (ATAC) and the RCMP. The decision record of the Committee described the threat to cargo:

... [T]he nature of the threat was changing and acts of sabotage rather than hijacking were perceived as the main threat to the safety of the air transportation system in the future. As passenger screening procedures have proven to be an effective deterrent to prevent the carriage of unauthorized

¹⁴⁷⁴ Exhibit P-411, p. 3.

¹⁴⁷⁵ Wallis, *Combating Air Terrorism*, p. 79.

¹⁴⁷⁶ Exhibit P-361, Tab 1, p. 9 of 12.

weapons and explosives in the aircraft cabin there is concern that persons are now attempting to exploit the weaknesses in the security system to place explosives in checked baggage, express parcel shipments, cargo and mail.¹⁴⁷⁷

According to Transport Canada, air cargo includes mail and packages, in addition to larger pallets and containers.¹⁴⁷⁸

In 1982, Transport Canada commissioned a study to review the adequacy of existing air cargo and baggage security policies. The Department requested recommendations for enhancing security if inadequacies were discovered.¹⁴⁷⁹ A July 1983 draft study report made recommendations to improve air cargo security.¹⁴⁸⁰ Draft air carrier regulations in circulation since 1982 also recognized the importance of protecting air cargo. The draft regulations required air cargo screening to prevent or deter the unauthorized carriage of weapons, explosives or incendiary devices in cargo on board aircraft. All unknown shippers were to be identified, and additional precautions were to be taken during high threat situations. These precautions might include searching all cargo by physical or electronic means, delaying shipments to ensure that specific aircraft cannot be targeted, or refusing to transport cargo.¹⁴⁸¹

It appears that Transport Canada had incorporated air cargo security into its inspection regime by 1983. The Department's Civil Aviation Security Inspection Checklist at the time, used to conduct tests of airport and air carrier security, included a section on cargo:

Cargo Security

32. Have procedures been established to assure that air cargo is accepted only from bona fide shippers?
33. Are cargo shipments controlled from time of acceptance until loaded aboard the aircraft to prevent unauthorized access and the introduction of explosives?
34. Are all suspect or unidentified shipments examined and cleared by a responsible employee of the air carrier prior to being loaded aboard the aircraft?¹⁴⁸²

In December 1983, Paul Sheppard, Director of Aviation Security for Transport Canada, conducted a passenger screening test at Toronto International Airport

¹⁴⁷⁷ Exhibit P-101 CAF0163, p. 5.

¹⁴⁷⁸ Exhibit P-189, p. 8.

¹⁴⁷⁹ Exhibit P-101 CAF0776, p. 1.

¹⁴⁸⁰ Exhibit P-101 CAF0565, pp. 10-11.

¹⁴⁸¹ Exhibit P-101 CAF0565, pp. 8-9.

¹⁴⁸² Exhibit P-101 CAF0566, p. 7.

using the Civil Aviation Security Inspection checklist, but did not pose these questions relating to air cargo security.¹⁴⁸³

Sheppard later reviewed Air India's security plan and, on February 21, 1984, accepted it as "...a commendable program that meets the requirements of Canadian legislation." The plan included measures for air cargo security under both normal and emergency conditions. In emergency conditions, all cargo was to be subject to a "cooling period" of 24 hours in the event of a bomb or sabotage threat.¹⁴⁸⁴

Transport Canada was aware of the security risk posed by air cargo, and evidence before the Commission demonstrates that industry stakeholders made the Department aware of inadequacies in security. In particular, the concern that small packages could be directed to specific flights was brought to Transport Canada's attention. In 1984, Transport Canada conducted a security audit of CP Air to assess its system for combatting acts of unlawful interference with civil aviation. Feedback from a Canadian Air Line Pilots Association (CALPA)¹⁴⁸⁵ security representative for CP Air indicated that "...CALPA would like to see better procedures in place for handling of checked baggage and cargo and believe that more can be done to help with searches, electronically or otherwise."¹⁴⁸⁶ Another security representative indicated:

CALPA are quite concerned about the lack of procedures in place for handling checked baggage, small parcels and cargo.... [I]t is quite conceivable to direct a small parcel to a specific flight. Neither the airlines nor Transport Canada have any large x-ray facilities in place at airports to handle checked baggage or cargo.¹⁴⁸⁷

By 1985, cargo was acknowledged as a distinct security risk and air carriers were responsible for applying security standards for cargo. The *Civil Aviation Security*

¹⁴⁸³ Air cargo security, while part of the checklist, was not assessed on this particular occasion. No answers had been provided to these questions in this particular review and a handwritten note beside each of these questions read "not checked," with no reason provided. It seems likely that cargo security was not assessed because the testing had focused on passenger screening. The fact nevertheless remains that Transport Canada considered cargo security to be of enough importance to include these questions as part of its general Inspection Checklist for civil aviation security. See Exhibit P-101 CAF0566.

¹⁴⁸⁴ Exhibit P-284, Tab 68, s. 8.1.4.

¹⁴⁸⁵ CALPA, though not defined in this document, appears to refer to the Canadian Air Line Pilots Association, which was formed in 1937. Its objective was "...to consolidate airline pilots' views regarding aviation concerns, with the authority to voice them when necessary." In 1996, the organization disbanded when Air Canada pilots formed their own organization, the Air Canada Pilots Association (ACPA). In 1997, the remaining members of CALPA arranged a merger with the US-based Airline Pilots Association (ALPA). See Exhibit P-412.

¹⁴⁸⁶ Exhibit P-101 CAF0637, p. 10.

¹⁴⁸⁷ Exhibit P-101 CAF0637, p. 14.

Measures Regulations and *Foreign Aircraft Security Measures Regulations* in place at the time required all air carriers to have manual, mechanical or electronic surveillance and search systems for cargo, and to provide for restricted areas for cargo at aerodromes.¹⁴⁸⁸ The Measures also required air carriers to establish "...a system of identification that prevents baggage, goods and cargo from being placed on board aircraft if it is not authorized to be placed on board by the owner or operator."¹⁴⁸⁹

In the first hours following the loss of Air India Flight 182, air cargo was identified as a priority risk to civil aviation that required immediate attention. On June 23, 1985, the Government implemented provisional security measures while awaiting further information that would help identify the more permanent changes needed. Among these stop-gap measures were a 24-hour hold on all cargo and a physical search or X-ray inspection.¹⁴⁹⁰

Even before the bombing of Flight 182, Transport Canada understood that cargo destined for aircraft needed protection from sabotage and that carrying of explosives in cargo was a specific risk.

3.8.1.1.1 The Seaborn Report

As a result of the Air India bombing, the federal Cabinet¹⁴⁹¹ commissioned a study to provide a holistic review of airport and airline security in Canada.¹⁴⁹² The report, known as the Seaborn Report, was released in late September 1985. It called for an improved national civil aviation security regime for air cargo and highlighted the need to protect likely targets of terrorism. It spoke of the importance of maintaining a rigorous security regime, even under normal threat levels.¹⁴⁹³

The Seaborn Report outlined a program for enhanced air cargo security at international airports. The program would vary according to the level of threat.¹⁴⁹⁴ Echoing the feedback received during Transport Canada's 1984 security audit of CP Air, the report recommended paying greater attention to small parcels because of their potential to target specific flights, and suggested that such parcels be X-rayed, even in normal threat situations.¹⁴⁹⁵

For instances of enhanced threat, the report recommended that, in addition to X-raying small parcels, larger cargo should undergo X-ray, physical or canine inspection, or be subject to a holding period that was not publicly disclosed. The report called for a complete ban on cargo during high threat periods or,

¹⁴⁸⁸ Exhibit P-165, Tab 4, ss. 3(1)(a), (b), (c); Exhibit P-165, Tab 5, ss. 3(1)(a), (b), (c).

¹⁴⁸⁹ Exhibit P-165, Tab 4, s. 3(1)(f); Exhibit P-165, Tab 5, s. 3(1)(f).

¹⁴⁹⁰ Exhibit P-35, p. 20; see also Testimony of Jean Barrette, vol. 37, May 31, 2007, p. 4509.

¹⁴⁹¹ Exhibit P-101 CAF0039, p. 1 of 10.

¹⁴⁹² Exhibit P-35, p. 20.

¹⁴⁹³ Exhibit P-101 CAF0039, p. 3 of 10.

¹⁴⁹⁴ Exhibit P-101 CAF0039, p. 6 of 10.

¹⁴⁹⁵ Exhibit P-101 CAF0039, p. 6 of 10.

alternatively, a refusal to ship cargo that could not be opened and thoroughly inspected.¹⁴⁹⁶

The report observed that "...[n]ew explosive vapour detection technology should be available within the next two to three years to speed up the checking of cargo."¹⁴⁹⁷ It urged Transport Canada to develop new technologies as a priority "...to assist in streamlining and improving the effectiveness of security detection techniques and equipment."¹⁴⁹⁸ The report noted that cargo screening would generally be done by air carriers or by private security firms acting on their behalf. It advised Transport Canada to set and enforce security standards and to ensure adequate training for those screening air cargo.¹⁴⁹⁹

The Seaborn Report was widely lauded as a seminal document in Canada and in the international aviation security community. It continues to resonate within the international community today.¹⁵⁰⁰ Jim Marriott, Director of Transport Canada's Aviation Security Regulatory Review at the time of the hearings, outlined the impact of the Seaborn Report domestically and internationally:

The Seaborn Report really became a strategic action plan for the Department for many years to follow. It outlined a large number of practices recommended to further enhance aviation security. And the Department very aggressively pursued implementation of all recommendations in the Seaborn Report over the course of the coming years, in conjunction with and in coordination with other federal government departments that had security responsibilities, and, of course, in conjunction and in coordination with the aviation industry, airlines, airports and labour groups within airports and airlines....

So it was really a roadmap to take aviation security in Canada from where it was in the aftermath of 1985 to a new and much higher ground....[N]ot only was it a significant report for Canadian aviation security but also for international aviation security.

...

...[T]he recommendations implemented by Canada became standards against or benchmarks against which international aviation security evolved and looked to.¹⁵⁰¹

¹⁴⁹⁶ Exhibit P-101 CAF0039, p. 6 of 10.

¹⁴⁹⁷ Exhibit P-101 CAF0039, p. 6 of 10.

¹⁴⁹⁸ Exhibit P-101 CAF0039, p. 6 of 10.

¹⁴⁹⁹ Exhibit P-101 CAF0039, p. 7 of 10.

¹⁵⁰⁰ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4507.

¹⁵⁰¹ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4504-4505.

Marriott's statement that all Seaborn's recommendations were aggressively pursued seemed at odds with Transport Canada actions relating to air cargo security. As discussed below, air cargo security measures were not implemented in the way recommended by Seaborn. For example, small parcels were not, and still are not, routinely X-rayed.¹⁵⁰² No routine search methodologies are used for such packages, despite ongoing concern that they may be used to target specific flights.¹⁵⁰³ In 2006, an independent panel of experts reported on its review of the *Canadian Air Transport Security Authority Act (CATSA Act)*. The CATSA Act Review Advisory Panel (CATSA Advisory Panel) noted that it was "...struck by the similarity of many of our recommendations ... to address deficiencies in aviation security to those of the Seaborn Report, some twenty years earlier."¹⁵⁰⁴ Only in very recent years has the need to address air cargo security appeared to gain currency with the Government of Canada.

Marriott testified that it would have been possible to act immediately to implement some of Seaborn's recommendations, but others required a number of years to put into place.¹⁵⁰⁵ More than two decades after the report was issued, however, air cargo remains a major gap in security. This is not an acceptable time frame to address a threat that profoundly endangers the lives of passengers and all those involved with aviation.

Senator Colin Kenny, Chair of the Senate Committee which has been monitoring aviation security in Canada in recent years,¹⁵⁰⁶ conveyed the Committee's profound concern about the time taken to address cargo security:

Well, we frankly were appalled when the Government announced approximately a year ago that it was commencing a study to determine how they were going to handle cargo in the hold.

It has been a long time since 9/11 and a much longer time since Air India and the Committee was appalled that the Government would just be starting to study this last year.

...

...I find it difficult to adequately express the frustration the Committee has with the slowness of the Department of Transport in addressing these issues.¹⁵⁰⁷

¹⁵⁰² Exhibit P-169, p. 52 of 202.

¹⁵⁰³ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4679.

¹⁵⁰⁴ Exhibit P-157, pp. 91-92 of 135.

¹⁵⁰⁵ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4506-4507.

¹⁵⁰⁶ Exhibit P-171, p. 151.

¹⁵⁰⁷ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4677.

3.8.1.1.2 Reasons for Inaction

Key to the Air India tragedies was the carriage of interlined baggage without an accompanying passenger, coupled with the failure to implement passenger-baggage reconciliation in the high-threat environment of June 1985. Yet Transport Canada was already well aware of the threat of bombs in suitcases and knew how to thwart this method of attack.¹⁵⁰⁸ A lack of vigilance in aviation security provided an opportunity for the bags to escape detection.

An analogous situation for air cargo has been allowed to persist for almost three decades. It is alarming that most cargo loaded onto passenger aircraft is still not subjected to inspection by X-ray or other means.

Why is this so? Transport Canada offered reasons related to the cost and complexity of appropriate security screening measures for air cargo. Time has been required to provide effective solutions. Yet this cannot explain a delay spanning decades.

The Senate Committee suggested that other factors may be at play. In its 2003 report on aviation security, the Committee recommended immediately starting random and targeted screening of air cargo.¹⁵⁰⁹ Transport Canada responded that a new initiative for cargo security was being developed in a manner that would "...mitigate security risks to aviation and facilitate the efficient movement of goods domestically and globally."¹⁵¹⁰ It further advised that "...Transport Canada's approach will seek to maintain the efficiency of the cargo and aviation industries while improving security."¹⁵¹¹ The Senate Committee was critical of this response, suggesting that business interests, in maintaining efficiency in the shipment of goods, were unduly interfering with cargo security. In 1993, Wallis wrote that airlines might be reluctant to invest in security measures for cargo because it might have an adverse impact on an important source of revenue.¹⁵¹²

It is a general principle of civil aviation that security must be balanced with efficiency.¹⁵¹³ Both the Senate Committee¹⁵¹⁴ and the Seaborn Report¹⁵¹⁵ recognized this. The goal of expeditiously moving passengers and baggage must be balanced with security concerns; the challenge is the same for cargo.¹⁵¹⁶ Stephen Conrad, Transport Canada's Project Director for Air Cargo Security, acknowledged that one of the current objectives with respect to cargo security is to ensure the continued efficient flow of goods.¹⁵¹⁷

¹⁵⁰⁸ Exhibit P-101 CAF0637, pp. 19-20.

¹⁵⁰⁹ Exhibit P-171, p. 55.

¹⁵¹⁰ Exhibit P-172, p. 41 of 155.

¹⁵¹¹ Exhibit P-172, p. 41 of 155.

¹⁵¹² Wallis, *Combating Air Terrorism*, p. 79.

¹⁵¹³ Exhibit P-169, p. 23 of 202.

¹⁵¹⁴ Exhibit P-172, p. 42 of 155.

¹⁵¹⁵ Exhibit P-101 CAF0039, p. 2 of 10.

¹⁵¹⁶ Exhibit P-169, p. 23 of 202; see also Exhibit CAF0039, p. 2 of 10.

¹⁵¹⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5187.

The air cargo industry, which includes courier services, is time-sensitive.¹⁵¹⁸ Some goods shipped as cargo, such as cut flowers and newspapers, can be rendered useless if delayed.¹⁵¹⁹ However, the Senate Committee stated that the interests of industry stakeholders must not trump necessary security measures.¹⁵²⁰

There is evidence before the Commission that, before 1985, passenger inconvenience was a factor in Air India's decision to switch from manual baggage matching procedures to X-ray scanning,¹⁵²¹ even though X-ray technology was in its infancy and was highly dependent on the skill of the operator to make it work, to the very limited extent it could.¹⁵²²

The CATSA Advisory Panel called leaving passenger and baggage screening to air carriers in the wake of the Air India bombings "...a serious weakness in the security system, as security would not be their primary concern."¹⁵²³ Nevertheless, Transport Canada decided to leave the responsibility with air carriers and to develop a strongly prescriptive regulatory regime, with improved training programs for screening personnel. The Panel observed that it was not until after September 11th that CATSA was created as a separate government authority "...to take on this crucial responsibility."¹⁵²⁴ Striking the right balance between efficiency and security has clearly been a perennial issue. The search to find that balance for air cargo must be informed by lessons from the past.

With the air cargo security gap already widely publicized¹⁵²⁵ and with a heightened threat from terrorists, all flights carrying cargo and originating in Canada are potential targets. Because there have been few incidents to date,¹⁵²⁶ complacency has set in. However, that complacency is misplaced. As discussed, a bomb hidden in air cargo caused an in-flight disaster in Canada many decades ago, and this component of aviation remains relatively unprotected from terrorist attack, while other aspects of civil aviation have benefited from significant improvements in security measures. Although often characterized as the "next threat," the possibility of bombs in air cargo is more aptly described as a long-recognized threat that has been left incompletely addressed. The risk of a bomb being introduced on an aircraft, although identified as the main aviation security concern since 1980, has never been treated seriously enough to trigger the rigorous preventive measures required.

The challenge is to design and sustain a robust regime for air cargo security before its weaknesses can be exploited. In 1985, the failure to implement adequate security measures to avert a known threat can be attributed, at least in part, to a culture of complacency.¹⁵²⁷ As Transport Canada itself acknowledged

¹⁵¹⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5203.

¹⁵¹⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5187.

¹⁵²⁰ Exhibit P-172, pp. 41-42 of 155.

¹⁵²¹ Exhibit P-101 CAF0581.

¹⁵²² Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4256-4257.

¹⁵²³ Exhibit P-157, p. 67 of 135.

¹⁵²⁴ Exhibit P-157, p. 67 of 135.

¹⁵²⁵ Exhibit P-35, p. 21; Exhibit P-172, p. 29 of 155; Exhibit P-169, p. 52 of 202.

¹⁵²⁶ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁵²⁷ Exhibit P-157, p. 54 of 135.

in a report prepared in 1982, aviation security and security measures to counter terrorism were given a low priority in Canada because such issues were not truly viewed as an immediate threat to Canada:

Complacency can be identified as a potential issue both at the senior management level and on sites. As Canada has not experienced an increase in unlawful acts directed against civil aviation it may well become more difficult to justify the continuation of an adequate security program in the absence of a clearly defined threat. Security costs are relatively easily identified and hence present clear potential for cost reduction in the continuing absence of a clearly perceived threat.¹⁵²⁸

3.8.1.1.3 Need for a Proactive Approach

The CATSA Advisory Panel concluded that a proactive, rather than reactive, approach was fundamental to effective aviation security.¹⁵²⁹ Historically, as noted, aviation security concerns have consistently been dealt with by reacting to events. Passenger screening came about as a result of aircraft hijacking incidents. Passenger-baggage reconciliation was implemented following the Air India bombing. Heightened screening measures for passengers and baggage resulted from the attacks of September 11th. Liquids and gels were restricted because of an immediate and urgent threat in August 2006.

Canada is not alone in implementing security measures as a reaction to aviation incidents. Both the bombings of Air India Flight 182 in 1985 and Pan American (Pan Am) Flight 103 in 1988 focused the international civil aviation community's attention. Even after these events, however, many states were slow to improve aviation security. Many measures proposed by the International Civil Aviation Organization (ICAO) were voluntary or were not adopted by member states.¹⁵³⁰ Complacency may not be unique to Canada, but this by no means absolves it of responsibility for its inaction on air cargo.

At the hearings, Dr. Kathleen Sweet, an international civil aviation security expert with particular experience in air cargo security, warned that the threat from air cargo is imminent and that definitive action is required:

...[U]nless we get on this quickly...a plane is going to go down. It is going to be in the cargo hold, and everybody is going to be fighting the next war. Well, why didn't we do this? Well, why didn't we do that?... We have the opportunity right now to do it.¹⁵³¹

¹⁵²⁸ Exhibit P-101 CAF0774, p. 22 of 98.

¹⁵²⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4646.

¹⁵³⁰ Exhibit, P-157, p. 91 of 135.

¹⁵³¹ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4958-4959.

Air cargo must undergo as vigilant a screening process as passengers and their baggage. The precise route taken to achieve that outcome may vary according to the context, circumstances and means available.

The same is true for air cargo on all-cargo flights. The CATSA Advisory Panel concluded that all-cargo flights posed less risk because they did not carry passengers, only a small crew was on board, and it was difficult for a terrorist hiding in the hold to access the crew from there. All-cargo aircraft were therefore relatively unattractive targets for terrorists,¹⁵³² who often aimed for the greatest number of victims.¹⁵³³ Still, large cargo aircraft have considerable fuel reserves and can be commandeered and used as suicide weapons or for the dispersal of biological or chemical weapons. The CATSA Advisory Panel did not see this threat to be as significant in Canada as that posed by cargo on passenger aircraft.¹⁵³⁴ Senator Kenny, on the other hand, argued that all-cargo aircraft were likely just as vulnerable to sabotage as passenger aircraft.¹⁵³⁵

Captain Jean Labbé, Security Coordinator for the National Security Committee of the Air Line Pilots Association, International (ALPA), summed up the concern with air cargo security:

Cargo is a big file for ALPA. There are steps that are being taken to improve security on board cargo aircraft. Are those measures being applied quickly enough? I don't think so. Are enough measures being introduced at this time? I don't think so, either.

I feel it's a file that must and should be a priority. Cargo aircraft are currently lacking in terms of security in comparison with passenger aircraft, and even with passenger aircraft that carry cargo, the cargo that is loaded and the way that cargo is monitored – is screened – is perhaps not up to the standards we'd like, which is comparable to the standards for baggage.¹⁵³⁶

3.8.1.2 International Developments in Air Cargo Security

Immediately following the Air India bombing, air cargo was identified as a risk. On June 28, 1985, in direct response to the loss of Air India Flight 182, IATA convened an extraordinary meeting of its Security Advisory Committee (SAC), which consisted of airline security chiefs from around the world. Representatives from several international airlines and civil aviation stakeholders attended, notably ICAO, Air India, CP Air, Air Canada and the Air Transport Association

¹⁵³² Exhibit P-169, p. 53 of 202.

¹⁵³³ Exhibit P-263, p. 15.

¹⁵³⁴ Exhibit P-169, p. 53 of 202.

¹⁵³⁵ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4683.

¹⁵³⁶ Testimony of Jean Labbé, vol. 64, October 23, 2007, p. 7992 [translation].

of Canada. Representatives from Transport Canada and the United States' Federal Aviation Administration (FAA) were present as well.¹⁵³⁷ Wallis, who had convened the meeting as Director of Security for IATA, noted the significance of delegates from Transport Canada and the FAA attending an "airline meeting." He said it was indicative of the level of interest that governments were taking in the issues.¹⁵³⁸

The issues discussed at the meeting eventually led to "massive changes" in civil aviation security. From this meeting, three working groups were established to address pressing aviation security issues.¹⁵³⁹ One was devoted to air cargo security.¹⁵⁴⁰

3.8.1.2.1 The Problem: Cargo Consignments can Target Specific Aircraft

Airline officials were aware of the risks that cargo presented and that changes occurring in the cargo industry increased those risks. For many years, it was not possible to identify the flight on which a cargo consignment would be loaded. This served as a built-in protection against terrorists wishing to attack a specific aircraft. However, it was increasingly becoming possible to identify the flight transporting a particular consignment.¹⁵⁴¹ This removed a "principal pillar" of airline defences against saboteurs.¹⁵⁴² In addition, freight companies were consolidating a wide range of small consignments into full aircraft containers, making it more difficult for airlines to ascertain the integrity of the load.¹⁵⁴³ The nature, size and volume of cargo all militated against the effective application of security controls at the airport.

Wallis testified that applying security controls to cargo at the airport was "too late" in any event.¹⁵⁴⁴ It was from the IATA deliberations that began in June 1985 that the concept of the "known shipper" developed.¹⁵⁴⁵ The working group on cargo security reported to the SAC at its next regular meeting in September 1985,¹⁵⁴⁶ building on the work at the June 28th, 1985 meeting.¹⁵⁴⁷

Transport Canada representatives attended the IATA meeting on June 28th. The Department must have known about the working groups formed at both IATA and ICAO to address air cargo security.

¹⁵³⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4474.

¹⁵³⁸ In the weeks preceding this meeting there had been a number of other aviation security incidents, including the hijacking of a TWA airplane in the Middle East, which had lasted for many days. Wallis, who was Director of Security at IATA at the time and had convened the extraordinary meeting, testified that "...it was the Air India incident which triggered the call for the meeting." See Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4474-4475.

¹⁵³⁹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4476.

¹⁵⁴⁰ Exhibit P-162, p. 4.

¹⁵⁴¹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4480-4481.

¹⁵⁴² Wallis, *Combating Air Terrorism*, p. 79.

¹⁵⁴³ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁴⁴ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5004.

¹⁵⁴⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

¹⁵⁴⁶ Exhibit P-162, p. 5.

¹⁵⁴⁷ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4494.

3.8.1.2.2 The Proposed Solution: “Known Shipper”

The solution to the threat posed by air cargo involved partners in the regular movement of cargo.¹⁵⁴⁸ The notion of the “known shipper” was a construct devised by the airlines to decentralize cargo security.¹⁵⁴⁹ Freight forwarders, consolidators and manufacturers who were regular cargo handlers would be required to apply security controls to cargo at their facilities and during transport to the air carrier. To prevent interference with airport-bound cargo, seals and other security controls would be applied to crates and vehicles upon loading. These would be removed only when the cargo was delivered to the air carrier or to its final destination.¹⁵⁵⁰ Applying security controls before air cargo arrived at the airport effectively “expanded” the outer perimeter of the airport to encompass the facilities of the freight forwarders, consolidators and manufacturers involved in the known shipper process.¹⁵⁵¹

It was not until 1989, however, that this approach gained currency at ICAO.¹⁵⁵² The bombing of Pan Am Flight 103 in December 1988, using the same ruses that led to the bombing of Air India Flight 182, brought renewed urgency to the issue.¹⁵⁵³ The United Kingdom assumed the lead role internationally on air cargo security. Wallis testified that the Pan Am bombing may have had greater effect than the Air India bombings on the UK because it involved a failure of security at a British airport, casualties had occurred on the ground and wreckage had fallen on dry land. The aircraft had “...blown up over Scotland and had rained death and destruction on the town of Lockerbie.”¹⁵⁵⁴

In 1989, the airlines began actively promoting the “known shipper” model for air cargo security and pushed for a formal known shipper procedure.¹⁵⁵⁵ In 1990, ICAO formed its own working group on air cargo security. The group consisted of representatives from the FAA and the UK Department of Transport, an airport representative and Wallis, who represented IATA. Wallis knew about IATA’s deliberations on this issue and was able to share these during the 1990 working group discussions.¹⁵⁵⁶ Wallis stated that the civil aviation authorities of the UK and the US “...quickly warmed to the principle” of the “known shipper,” recognizing that such a system would facilitate securing air cargo against potential terrorists.¹⁵⁵⁷ Marriott, who had joined Transport Canada’s security operations in 1986,¹⁵⁵⁸ described the UK as a leading advocate, aggressively pursuing enhancements for air cargo security on the international stage.¹⁵⁵⁹ The

¹⁵⁴⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5004.

¹⁵⁴⁹ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁵⁰ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5004-5005.

¹⁵⁵¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5004.

¹⁵⁵² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

¹⁵⁵³ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4529.

¹⁵⁵⁴ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4525.

¹⁵⁵⁵ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁵⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4481.

¹⁵⁵⁷ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁵⁸ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4484.

¹⁵⁵⁹ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4529.

US and UK civil aviation authorities and the world's airlines started promoting the concept of the "known shipper" within ICAO.¹⁵⁶⁰

At the time, IATA defined the "known shipper" as "...an approved agent, freight forwarder, account holder or other entity who has conducted business with carriers on a regular basis and has provided an acceptable security program to the appropriate authority."¹⁵⁶¹ According to Wallis, the "known shipper" could only be so designated if it was "known" to *both* the regulatory authority and the air carrier.¹⁵⁶² The former requirement was fulfilled if the entity was licensed by government, maintained a government-endorsed security program, possessed the ability to screen cargo and was monitored through government inspections. The latter requirement was satisfied if the entity had engaged in regular business with the air carrier, demonstrating a history of involvement.¹⁵⁶³

The ICAO working group on cargo security proposed adopting the "known shipper" concept to the Aviation Security Panel (AVSEC Panel) in April 1990, but was not successful. Member states expressed concern about the difficulties in implementing such an approach. Wallis attributed this lack of endorsement to the "lowest common denominator" or consensus model of decision-making followed by ICAO.¹⁵⁶⁴ It could be difficult for ICAO member states to reach agreement because they had widely disparate priorities and resources.

In 1991, however, IATA submitted a further proposal to the AVSEC Panel, calling for changes to Annex 17, the security annex to the *Convention on International Civil Aviation* ("*Chicago Convention*"), including the establishment of a definition for the "known shipper."¹⁵⁶⁵ Supported by proponents from the UK and US, the AVSEC Panel was persuaded to adopt the "known shipper" concept and to formally incorporate appropriate language into Annex 17.¹⁵⁶⁶ Marriott testified that "...the United Kingdom representative on the ICAO Aviation Security Panel, together with Mr. Wallis, were I think firm anchors in advancing the definition of a concept, a new...more enhanced concept for air cargo security that eventually became part of the international regulatory framework and has trickled down into international air cargo security programs."¹⁵⁶⁷

Wallis noted that such a system may have been difficult for developing nations to implement at the time, but that the developed world had the resources and the capability to do so. The UK moved swiftly to establish a "known shipper" system. By 1993, two years after ICAO accepted the concept, the UK produced aviation security regulations to govern the responsibilities of air cargo agents under its air cargo security program.¹⁵⁶⁸ Dr. Reg Whitaker, Chair of the CATSA Advisory

¹⁵⁶⁰ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁶¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5002-5003.

¹⁵⁶² Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

¹⁵⁶³ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5002-5003.

¹⁵⁶⁴ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

¹⁵⁶⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5002.

¹⁵⁶⁶ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁶⁷ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4529.

¹⁵⁶⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

Panel, which had the opportunity to examine the UK air cargo security system, called it “very impressive.”¹⁵⁶⁹ Another Panel member, Chern Heed, testified that the UK system included the regular inspection and certification of the entire chain of cargo handlers, starting with the shipper.¹⁵⁷⁰

Writing in 1993, Wallis remarked that “[w]ith so much freight being carried on passenger aircraft, it can be only a matter of time before other governments follow the front runners and adopt similar approaches to the question of cargo security.”¹⁵⁷¹ A number of European countries have introduced such air cargo security programs. The Netherlands and Ireland, for example, have both adopted sound security programs for air cargo in which security controls are administered prior to the cargo’s arrival at the airport. The agents who administer the controls are subject to inspection.¹⁵⁷²

3.8.1.3 Canada’s Existing Air Cargo Security Regime

3.8.1.3.1 Lack of Vigilance: “Known Shipper” Misconstrued

Although the current Canadian air cargo security program employs the term “known shipper,” the definition does not conform to the common international understanding of the term. Unlike the air cargo security programs in Europe, and unlike the definition sanctioned by the international regulatory regime, the term “known shipper” in Canada does not refer to a formally regulated, government-certified entity applying security controls to cargo at points away from the airport. There is no requirement in Canada for a “known shipper” to be “known” to government. Rather, the term simply refers to a shipper or freight forwarder “known” to an air carrier because the two have conducted business in the past.¹⁵⁷³

The precise definition of “known shipper” in Canada is contained in confidential regulations and measures. However, a publicly-accessible definition was discovered by counsel for the Flight 182 victims’ families in correspondence between the courier company Purolator, owned by Canada Post Corporation, and the CATSA Act Review Secretariat. Allegedly based on the definition contained in the confidential regulations and measures, “known shipper” was defined as an entity that “...has shipped on at least three accessions [*sic*] during the preceding six-month period.”¹⁵⁷⁴ Under cross-examination, Yves Duguay, Senior Director of

¹⁵⁶⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4630.

¹⁵⁷⁰ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4630.

¹⁵⁷¹ Wallis, *Combating Air Terrorism*, p. 78.

¹⁵⁷² Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4951; Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5192.

¹⁵⁷³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5293.

¹⁵⁷⁴ Exhibit P-191, p. 2.

Security at Air Canada during the Commission hearings, agreed that this closely approximated the official definition.¹⁵⁷⁵

Dr. Jacques Bourgault, one of the three members of the CATSA Advisory Panel, testified about how the known shipper concept was explained to him when he met with Air Canada representatives:

Well, we know the people around and they are known because we know them and if we don't know them, we apply the other rule which is that you withhold the parcel for a minimum of 24 hours.¹⁵⁷⁶

Under Canada's current air cargo security program, known shippers are not required to secure cargo either at their premises or during conveyance to the air carrier. There is no requirement for known shippers to conduct employee background checks.¹⁵⁷⁷ Once an air carrier confirms the "known" status of the shipper, the carrier can accept the cargo for transport on aircraft, with no obligation on the carrier to conduct further screening.¹⁵⁷⁸ Any screening of air cargo by X-ray or other means lies at the discretion of the air carrier.¹⁵⁷⁹ Air cargo received from unknown shippers is subject to a delay period to prevent an unknown shipper targeting a specific flight.¹⁵⁸⁰ In the United States, in contrast, air cargo originating from unknown shippers is not allowed on passenger aircraft.¹⁵⁸¹

Because Canada imposes few or no requirements for the physical screening of cargo, either before or after its acceptance, there can be no assurance that air cargo is safe. The fact that an entity has shipped cargo without incident on three previous occasions simply does not provide sufficient assurance that future air cargo shipments are safe. The reality is that almost 80 per cent of air cargo in Canada is transported by passenger aircraft,¹⁵⁸² that the aviation industry, and air carriers in particular, are attractive targets for terrorists,¹⁵⁸³ and that air cargo is a recognized vehicle for bringing bombs onto aircraft. Without screening,

¹⁵⁷⁵ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5296. Counsel for the Attorney General objected to the disclosure of this information on the basis that it "may enable persons to attempt to qualify as known shippers, to fall within that definition, and therefore get around the security controls": Sandy Graham, Counsel for the Attorney General of Canada, vol. 43, June 14, 2007, p. 5295. Counsel for the families indicated that this document had been obtained from Transport Canada's own website: Raj Anand, Counsel for the Family Interests Party, vol. 43, June 14, 2007, p. 5292. The Commission has concluded that this information has already been available in the public domain and discussion of its content was relevant in understanding the current state of air cargo security; see also Submissions of the Family Interests Party, paras. 74-75.

¹⁵⁷⁶ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4651.

¹⁵⁷⁷ Exhibit P-171, p. 48.

¹⁵⁷⁸ Exhibit P-171, p. 48.

¹⁵⁷⁹ Exhibit P-169, p. 52 of 202.

¹⁵⁸⁰ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5257-5258.

¹⁵⁸¹ Exhibit P-415, p. 30494.

¹⁵⁸² Exhibit P-169, p. 53 of 202.

¹⁵⁸³ Exhibit CAF0039, p. 3 of 10.

satisfying a single criterion – three previous shipments without incident – cannot ensure that air cargo poses no danger.

Twenty-first century terrorists are often well-educated and well-financed.¹⁵⁸⁴ It is easy to imagine them manipulating the existing air cargo security regime in Canada to achieve their ends. Nick Cartwright, Director of the Security Technology Branch at Transport Canada, explained that, in combating air terrorism, it is necessary to continue to “fight the last war,” but there is a need to look forward constantly to “...the next threat that is going to emerge.”¹⁵⁸⁵ Engaging in such contemplative exercises is fundamental to aviation security, according to Wallis: “We’ve got to think in those terms if we’re going to anticipate what they might do next. Then we can develop defences against what they might do next.”¹⁵⁸⁶

The Commission’s concern is that air cargo has been recognized as the “next threat” for almost thirty years. This concern deepens because of the ease with which a shipment can be used to target a specific flight. Senator Kenny testified that, despite airline claims to the contrary, cargo can target a specific flight, particularly in locations where flights are more predictable – for example, cities that have only infrequent flights to a particular destination – or where packages are delivered to an airport shortly before the final flight of the day to a given city.¹⁵⁸⁷ Wallis also maintained that, with courier traffic, “...the potential to target a specific airline is there. That loophole still has to be closed....”¹⁵⁸⁸ He had raised this same concern more than a decade earlier.¹⁵⁸⁹

The evidence before the Commission shows a long-standing concern about terrorists using cargo to target specific flights. Airline pilots working for CP Air cited this as a problem as early as 1984.¹⁵⁹⁰ The Seaborn Report, released in September 1985, drew particular attention to small packages and recommended possibly routinely X-raying them, even under normal threat conditions.¹⁵⁹¹

Testimony before the Senate Committee in 2002 about the ease with which air cargo could be used to transport bombs was compelling. Chuck Wilmink, a former Manager of Corporate Security for Canadian Airlines, offered his insights on the matter:

¹⁵⁸⁴ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

¹⁵⁸⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5231.

¹⁵⁸⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

¹⁵⁸⁷ Testimony of Colin Kenny, vol. 38, June 1, 2007, pp. 4679-4680; Kenny cited evidence presented before the Standing Senate Committee for National Security and Defence which “...came from a former airline security officer and he said by process of deduction it wasn’t hard to figure out where it was likely to go, that airlines tended to want to move things through in an expeditious way and so there would not be a 100 percent certainty but the odds would be in favour” of a package being loaded on a certain flight.

¹⁵⁸⁸ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

¹⁵⁸⁹ Wallis, *Combating Air Terrorism*, p. 79.

¹⁵⁹⁰ Exhibit P-101 CAF0637, p. 14 of 22.

¹⁵⁹¹ Exhibit P-101 CAF0039, p. 6 of 10.

...The current status of airport security is not very good. I could take anyone in this room and in two minutes train that person on how to put a bomb on an airplane for any city in the world. If you are willing to pay the first-duty shipping fee, we can guarantee what flight you will be on – it is that wide open....¹⁵⁹²

Although precautions such as minimum holding periods are in place for unknown shippers, such shippers account for only about 5 to 10 per cent of Canada's overall shipments, and represent a small fraction of the cargo industry in Canada.¹⁵⁹³ More than 16,000 entities fall into the "known shipper" category.¹⁵⁹⁴ No evidence was produced at Commission hearings to provide any assurance that known shippers are prevented from targeting specific flights. On the contrary, Wallis reported in 2003 that there was a general tendency in the airline industry to "...sell cargo hold capacity on specific flights."¹⁵⁹⁵

Whitaker was highly critical of the current system:

Well, simply we have a system in place now which is...the largely discredited notion of known shippers, which simply means that companies that are...regular shippers have their goods accepted, and there is no inspection regime to determine how secure their...facilities are.¹⁵⁹⁶

Wallis testified that the term "known shipper" was a misnomer. ICAO eventually began to use the term "regulated agent."¹⁵⁹⁷ Annex 17 of the *Chicago Convention* defines the term as follows:

An agent, freight forwarder or any other entity who conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo or mail.¹⁵⁹⁸

Wallis criticized Canada's interpretation of the known shipper concept:

¹⁵⁹² Exhibit P-171, p. 53.

¹⁵⁹³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5261.

¹⁵⁹⁴ Final Submissions of the Attorney General of Canada, Vol. II, para. 360.

¹⁵⁹⁵ Wallis, *How Safe Are Our Skies?*, p. 111.

¹⁵⁹⁶ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4630.

¹⁵⁹⁷ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

¹⁵⁹⁸ Exhibit P-181, Annex 17, p. 1-1.

...Now I've seen lots of things relative to known shippers in Canada and I believe that the interpretation of known shipper in the Canadian sense is totally wrong and it needs to be looked at again.

That language has changed and we now talk about regulated agents.... [T]he ideas that were developing in the early 90's were that we would regulate agents who [were] a) known to the airlines, but b) known to the governments. We would regulate them so that they would operate security programs within their own sheds.¹⁵⁹⁹

The United States has used a system of "known shippers" similar to Canada's system. The Known Shipper program has been described as a "fundamental element" of air cargo security in the United States since 1976, and has only recently been codified with the publication of the Final Rule on Air Cargo Security Requirements in May 2006.¹⁶⁰⁰ The Known Shipper program has been the "primary approach" for ensuring air cargo security and complying with legislation in the United States.¹⁶⁰¹

The US Known Shipper program was created to establish procedures for differentiating between shippers that are known and unknown to air carriers or freight forwarders, who act as intermediaries between shippers and carriers.¹⁶⁰² Shippers with "established business histories" with either air carriers or freight forwarders are permitted to ship their cargo on aircraft.

Following September 11th, the US Transportation Security Administration (TSA), the body with immediate responsibility for aviation security, issued directives requiring passenger carriers to transport cargo only from shippers that met certain eligibility criteria. However, in 2005, the US Government Accountability Office reported that local TSA officials at airports and numerous industry stakeholders had expressed concern about the Known Shipper program. The report stated that, while the "...program may provide some security benefit, it is by itself an insufficient security safeguard and must be supplemented by other security measures."¹⁶⁰³ It continued that the TSA requirements may not adequately deter or prevent terrorists from meeting basic eligibility criteria and becoming Known Shippers.¹⁶⁰⁴

3.8.1.3.2 Canada Falls Behind

Wallis suggested that Europe has always been ahead of North America in aviation security because of its history of involvement with terrorism. For this reason, he

¹⁵⁹⁹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4249.

¹⁶⁰⁰ Exhibit P-415, p. 30499.

¹⁶⁰¹ Exhibit P-416, p. 8.

¹⁶⁰² Exhibit P-416, p. 31.

¹⁶⁰³ Exhibit P-417, p. 32.

¹⁶⁰⁴ Exhibit P-417, p. 32.

argued, there was always a more pressing need to move forward with security measures in Europe.¹⁶⁰⁵ However, as the Air India bombing and the September 11th events showed, no region of the globe is immune to terrorism.

In its Final Submissions to the Commission, the Attorney General of Canada stated that the Government has a long-standing policy of commitment to "...a regulatory regime, which meets and in many areas exceeds the international benchmarks set by ICAO."¹⁶⁰⁶ It cited Canada's leading role in passenger-baggage reconciliation as an example. The submission cited Wallis, who had acknowledged that Canada was "at the forefront" in this effort,¹⁶⁰⁷ and that Canada had "pushed very hard" to take this issue forward at ICAO, because it had "...been hurt, obviously, by the bombing" of Air India Flight 182.¹⁶⁰⁸ Yet, air cargo security, which had also been identified as an issue after the Air India bombings, has remained virtually unimproved since 1980. In air cargo security, Canada does not meet international standards.

One of the key lessons from the Air India tragedies is that security depends on using layered measures to produce an acceptable level of protection against each vulnerability. To address one vulnerability while leaving another entirely untouched leaves a serious security gap. The current approach to air cargo security has created such a gap. In its 2007 report, the Senate Committee concluded that the "known shipper" system in Canada actually lessens aircraft security.¹⁶⁰⁹ Chern Heed, on behalf of the CATSA Advisory Panel, also had strong criticism of the program: "...There is a concept called the known shipper but to our minds it's not acceptable."¹⁶¹⁰

By 1991, the Government of Canada was fully aware of the air cargo security gap. Almost two decades later, this gap remains.

3.8.1.3.3 Voluntary Programs

Duguay testified about voluntary certification programs that involve security enhancements for goods crossing the Canada-US border. He testified as well that many of the large freight forwarder and shipping companies had voluntarily implemented security programs at their premises.¹⁶¹¹ As much as 80 per cent of Air Canada's cargo shipments is derived from the large freight forwarders and other large companies with whom Air Canada has a contractual relationship.¹⁶¹²

¹⁶⁰⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

¹⁶⁰⁶ Final Submissions of the Attorney General of Canada, Vol. II, para. 299.

¹⁶⁰⁷ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4755; see also Final Submissions of the Attorney General of Canada, Vol. II, para. 301.

¹⁶⁰⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4477; see also Final Submissions of the Attorney General of Canada, Vol. II, para. 300.

¹⁶⁰⁹ Exhibit P-172, p. 64 of 155.

¹⁶¹⁰ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4650.

¹⁶¹¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5296.

¹⁶¹² Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5251.

There was little testimony about voluntary programs, but this issue merits discussion. Voluntary border security programs that are limited to trade with the United States and that are based on goodwill¹⁶¹³ or external certification by the DHS,¹⁶¹⁴ do not provide assurance that adequate security procedures will consistently be applied to air cargo. Such programs amount to a “soft” form of regulation and are reminiscent of the regime in place for monitoring air carrier security plans in 1985. At the time, if there were concerns with an air carrier’s security plan, Transport Canada could notify the carrier but had no authority to take action.¹⁶¹⁵ Without effective enforcement mechanisms, there can be no assurance of security. As well, regional arrangements leave gaps.

Canada should also not rely on external certification programs for the security of air cargo originating from Canadian sources. This is a national security concern. Relying on foreign certification processes outsources the responsibility for protecting national security.

Some shippers and freight forwarders may have their own cargo security programs, but these voluntary programs in no way solve the problem of air cargo security. Where plans are voluntary, compliance is often inadequate.¹⁶¹⁶ Voluntary programs cannot ensure the quality or adequacy of security measures for the threat being addressed, and any monitoring in the absence of a formal regulatory arrangement is meaningless, since compliance with measures cannot be enforced.

Sweet criticized voluntary measures in the United States, particularly in air cargo security. She testified that compliance could not be guaranteed “...because security is often the bottom line budget item.”¹⁶¹⁷ As profit-seeking entities facing competing interests, businesses may limit the security measures they choose and apply them inconsistently.

The lessons of history cannot be ignored. The Commission heard how, on June 22, 1985, the Linescan II X-ray machine for checked baggage was not available in Toronto. Instead, Air India used the PD-4 “sniffer,” despite being informed of its ineffectiveness in detecting explosives.¹⁶¹⁸ The evidence suggests that economic considerations and time constraints in a customer-oriented business environment influenced the decision not to engage in manual methods of

¹⁶¹³ The Partners in Protection program, administered by the Canada Border Services Agency (CBSA), “enlists the cooperation of private industry to enhance border and trade chain security.” As such, the program urges members to improve their physical, infrastructural and procedural security. The program involves an arrangement “based on goodwill” that addresses security enhancements through self-assessments, with the goal of minimizing the threat of illegal activity. See Exhibit P-414.

¹⁶¹⁴ The Customs and Trade Partnership Against Terrorism (C-TPAT) program in the United States enables shippers, freight forwarders and air carriers to apply to become certified for the purpose of facilitating trade across the border. Certification in C-TPAT is based on an accreditation process in which a security program is required. At the moment, certification in C-TPAT is provided by the Department of Homeland Security (DHS), but this function may be outsourced to third parties in the future.

¹⁶¹⁵ Exhibit P-157, p. 66 of 135; see also Exhibit P-101 CAC0517, p. 5 of 5.

¹⁶¹⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4948.

¹⁶¹⁷ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4948.

¹⁶¹⁸ Exhibit P-157, p. 61 of 135

passenger-baggage reconciliation and physical inspection of baggage, even in light of the security threat at the time.

In a November 1984 memorandum, Sheppard noted the difficulties experienced by Transport Canada in assisting the air carriers to meet their security requirements for checked baggage and small freight:

Continuing need for high level security for certain airlines such as Air India. Baggage matching was so time consuming and leading to loss of confidence on the part of the passengers that Air India has leased a large scan ray unit for Mirabel.¹⁶¹⁹

Programs for air cargo security must be regulated so that all comparable entities face the same requirements, including meaningful oversight and enforcement. The regulated agent program approved by ICAO and, by inference, approved by Canada as a member state of ICAO, is an example of a global program that effectively addresses the threat posed by air cargo.

3.8.1.3.4 Inadequate Cargo Screening

Note on Terminology

One issue that must be addressed is precision in terminology. The terms “screening,” “searching” and “inspecting” were used in reference to air cargo security, often in a seemingly interchangeable manner. When the Commission sought to better understand these terms, differences in interpretation became apparent. This was of concern, since confusion over the meanings of these terms could impact cargo security.

Conrad described “screening” as a broad term that encompasses all methods of validating and verifying cargo, including “searching” and “inspecting” cargo. He described “searching” and “inspecting” as equivalent terms that refer to the examination of cargo by physical, X-ray, trace, canine and other such means.¹⁶²⁰ These methods were considered “active” forms of security screening.¹⁶²¹ He viewed “searching” and “inspecting” as a sub-component of the global term “screening.”¹⁶²²

On the other hand, Duguay stated that the current aviation security regime distinguished between “screening” and “searching.” He described “screening” as simply referring to the process by which air carriers accept cargo from shippers or freight forwarders. This involved an assessment of specific security indicators,

¹⁶¹⁹ Exhibit P-101 CAF0581, p. 1.

¹⁶²⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5191; see also Exhibit P-101 CAF0872, p. 3.

¹⁶²¹ Conrad described “passive” forms of screening as including, for example, the use of holding periods or decompression chambers. See Exhibit P-101 CAF0872, p. 2.

¹⁶²² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5191.

such as the size, description and source of a cargo shipment, to determine whether it raised any security concerns. Cargo from an unknown shipper, for example, required more stringent security controls. Only an air carrier employee with extensive training in the security indicators linked to cargo acceptance was allowed to perform this task.¹⁶²³

Conrad's description of screening would include the process of cargo acceptance, as described by Duguay. Throughout the Commission's hearings on aviation security, experts and industry stakeholders, including Duguay, frequently used air cargo "screening" in a sense that incorporated "searching" and "inspecting."¹⁶²⁴ This appears to be consistent with the definitions of "screening" found in the *Aeronautics Act* and in the *Canadian Aviation Security Regulations*. Although the definition in the Regulations refers only to passengers, baggage and vehicles, the definition in the Act applies to aviation security generally.¹⁶²⁵

There also appears to be confusion about these terms in the United States.¹⁶²⁶ The TSA considers "inspection" to be a subset of "screening," according with Conrad's interpretation of these terms.¹⁶²⁷

It seems that the broad conceptualization of the term "screening" is part of common industry parlance, and finds support in legislation. For clarity, however, greater precision and conformity is necessary.¹⁶²⁸ With respect to cargo, this Report considers the term "screening" as pertaining to all methods of validation

¹⁶²³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5254.

¹⁶²⁴ Exhibit P-169, p. 48; Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5291.

¹⁶²⁵ *Aeronautics Act*, s. 4.7: "screening" means a screening, including a search, carried out in the manner and under the circumstances prescribed in aviation security regulations, security measures, emergency direction or interim orders; *Canadian Aviation Security Regulations*, SOR/2000-111, s. 1: "screening" means the checking, identification, observation, inspection or authorized search of persons, goods and other things in the possession or control of persons who are screened and vehicles under the care or control of persons who are screened to prevent the carrying or transport, contrary to these Regulations, of weapons, explosive substances, incendiary devices or their components or other dangerous items that could be used to jeopardize the security of an aerodrome or aircraft: Exhibit P-176.

¹⁶²⁶ Comments submitted to the Transportation Security Administration following the publication of the Notice of Proposed Rulemaking (NPRM) on November 10, 2004, regarding proposed air cargo regulations in the United States included questions about the distinction between the terms "inspect" and "screen." See Exhibit P-415, p. 30484.

¹⁶²⁷ The TSA defines "screening" as a broad term referring to the "...systematic evaluation of a person or property to assess whether either poses a threat to security." The term "inspection" is considered a subset of "screening," since it is a method of conducting such an evaluation, but is not the only means of doing so. The known shipper program in the United States, for example, is considered an "information-based" method of screening, since it involves screening of cargo using information that is known about the shipper. As such, the TSA has advised that the terms "inspection" and "screening" are not interchangeable. See Exhibit P-415, p. 30484.

¹⁶²⁸ In a 2005 report on air cargo security, the United States Government Accountability Office also emphasized the need for clearer definitions for "screening" and "inspection" in order to ensure the appropriate type of inspection is conducted for air cargo. The report contended that the Transportation Security Administration (TSA) used the terms interchangeably, creating confusion among stakeholders about the actions they were required to take in examining air cargo. In particular, it was noted that some stakeholders were unsure whether "inspection" meant conducting a physical search, and whether "screening" meant the use of non-intrusive methods such as X-ray machines. See Exhibit P-417, p. 63.

and verification, including “searching” and “inspecting,” as well as to cargo acceptance as outlined by Duguay. The more specific terms will be used here, where appropriate. The terms “searching” and “inspecting” refer to active forms of cargo screening.

Minimal Searching of Air Cargo

Air cargo is not routinely searched prior to being placed aboard aircraft.¹⁶²⁹ Under the current legislation, the responsibility for searching air cargo by X-ray or other means lies with the air carrier.¹⁶³⁰ The searching is done at the air carrier’s discretion,¹⁶³¹ or in circumstances specified by the confidential *Air Carrier Security Measures*. The air carrier may contract with another agency to perform this work on its behalf.¹⁶³²

In the US, the DHS reported that most cargo carried on passenger aircraft is not physically screened or inspected.¹⁶³³ Legislation enacted in 2005, however, required the TSA to increase the percentage of cargo destined for passenger aircraft that had to be inspected.¹⁶³⁴ In August 2007, legislation was enacted to require 100 per cent screening by 2010.

In Canada, cargo from unknown shippers is subject to a delay before being carried on aircraft, but cargo from known shippers is accepted for immediate transport.¹⁶³⁵ Known shippers account for most of the cargo carried on passenger aircraft,¹⁶³⁶ yet there is no requirement that these entities secure cargo before its arrival at the airport, and the shippers themselves are subject to little scrutiny.

Lack of Technological Equipment

Legislation provides for air carriers to employ technical equipment for searching cargo, but Duguay testified that Air Canada does not have access to such equipment at airports in Canada.¹⁶³⁷ This was startling testimony from the Director of Security for the nation’s largest airline, especially given the Seaborn Report’s recommendation almost a quarter century ago for technology to be employed to screen air cargo.

Even before the Seaborn Report, industry participants had identified the lack of X-ray facilities for handling cargo at airports as a security gap. The main concern was the potential for small parcels to target specific flights. This concern was brought to Transport Canada’s attention no later than November 1984.¹⁶³⁸ In

¹⁶²⁹ Exhibit P-169, p. 52 of 202.

¹⁶³⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5188.

¹⁶³¹ Exhibit P-169, p. 52 of 202.

¹⁶³² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5188.

¹⁶³³ Exhibit P-417, pp. 1-2.

¹⁶³⁴ Exhibit P-417, p. 2.

¹⁶³⁵ Exhibit P-169, p. 53 of 202.

¹⁶³⁶ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5261.

¹⁶³⁷ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5291

¹⁶³⁸ Exhibit P-101 CAF0637, p. 14 of 22.

November 1984, Sheppard appeared to consider using X-ray equipment to screen cargo in some circumstances. In an internal Transport Canada memorandum, Sheppard suggested that X-ray units, which had already been deployed at some airports in the United States, might provide a solution for securing both checked baggage and small freight. He proposed purchasing mobile “scan ray” units for Transport Canada’s major facilities and specified that the units should have openings large enough to accommodate small cargo.¹⁶³⁹

It is clear that the use of X-ray equipment for screening cargo was contemplated before 1985. It was recommended by the Seaborn Report, as were other methods for searching cargo. By 2007, however, Canada’s largest airline still did not have access to X-ray machines or any other technology for searching cargo. This conflicts with the assessment by Marriott in his testimony that Transport Canada had “aggressively pursued” all the Seaborn recommendations.¹⁶⁴⁰

Challenges in Searching Air Cargo

Cartwright and Conrad both saw developing a program for air cargo screening as challenging. They testified that air cargo screening is more complex than either passenger or baggage screening because of the multiple variable characteristics of cargo. The size, content and makeup of passengers and baggage are predictable to some degree; this is not the case for much air cargo. Passenger baggage, for example, must comply with size and weight restrictions. Since bags are always notionally “attached” to passengers, they tend to contain similar items.¹⁶⁴¹ There is no such consistency with air cargo shipments.

Air cargo is highly diverse,¹⁶⁴² consisting of any commodity that can be shipped by air, from livestock¹⁶⁴³ to fresh produce¹⁶⁴⁴ to large machinery.¹⁶⁴⁵ Cargo is often consolidated into large containers and pallets, making searches difficult. The smallest packages are the simplest to screen.¹⁶⁴⁶ Although better means to screen pallets are being developed, the most effective screening occurs when cargo is in small containers. As a result, the best time to use technology to search cargo is before it is consolidated with other cargo in a large container.¹⁶⁴⁷

The greater volume of cargo compared to passenger baggage also presents a challenge for screening,¹⁶⁴⁸ as do the urgent time frames surrounding certain types of cargo, such as fresh seafood and cut flowers.¹⁶⁴⁹ Air cargo screening must also contend with geographic variability. Particular types of cargo, such

¹⁶³⁹ Exhibit P-101 CAF0581, p. 2.

¹⁶⁴⁰ Testimony of Jim Marriott, vol. 37, May 31, 2007, p. 4504.

¹⁶⁴¹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5151.

¹⁶⁴² Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5233.

¹⁶⁴³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5261.

¹⁶⁴⁴ Exhibit P-417, p. 9.

¹⁶⁴⁵ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5198.

¹⁶⁴⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5203.

¹⁶⁴⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5201.

¹⁶⁴⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5233.

¹⁶⁴⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5180-5181.

as fresh or frozen fish, are concentrated in certain locations. Not all screening equipment works equally well with all types of cargo.¹⁶⁵⁰ Part of the difficulty in deciding which screening technology to employ stems from the wide variance in the types of cargo being shipped from different locations across the country.¹⁶⁵¹

Cartwright testified about the importance of matching technology to the type of cargo to ensure that screening is effective and not merely perfunctory.¹⁶⁵² This is a critical endeavour. One of the most important lessons from the bombing of Air India Flight 182 was to avoid the merely cosmetic use of technology.¹⁶⁵³

Lagging Technological Advancement

Despite the challenges in searching air cargo, it appears that much of the developed world has long embraced technological means for doing it. In 1990, the production of mass spectrometry equipment and research into thermal neutron analysis techniques were accelerated for the purpose of screening air cargo.¹⁶⁵⁴ Yet in 2007, Transport Canada advised that it was only just considering some of these techniques.¹⁶⁵⁵ In 1993, X-ray manufacturers had already for some time been refining products for handling bulk containers.¹⁶⁵⁶ However, Transport Canada informed the Commission that technologies for screening consolidated, or bulk, cargo were still in the development stages.¹⁶⁵⁷

In 2003, Wallis argued that the required technology for screening air cargo was available and had been deployed “in airlines’ cargo warehouses.” He also reported that mass spectrometry and other vapour analysis systems for handling bulk shipments had already “proved their potential,” and that “hi-tech” screening devices had been developed and were positioned in airline cargo warehouses around the world:

Cargo security has moved with, and in some cases ahead of, the times. Hi-tech defenses have been harnessed to take air cargo security into the twenty-first century.¹⁶⁵⁸

Testimony at the Commission hearings supported the contention of Wallis that the technology for searching cargo exists. Air Canada employs X-ray machines to search cargo in other countries that require such searches. For example, X-ray machines have been positioned at Air Canada’s cargo hangars in London

¹⁶⁵⁰ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5151.

¹⁶⁵¹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5180-5181.

¹⁶⁵² Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5180-5181.

¹⁶⁵³ Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 5256-5257.

¹⁶⁵⁴ Wallis, *Combating Air Terrorism*, p. 78.

¹⁶⁵⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5181.

¹⁶⁵⁶ Wallis, *Combating Air Terrorism*, p. 78.

¹⁶⁵⁷ Final Submissions of the Attorney General of Canada, Vol. II, para. 363.

¹⁶⁵⁸ Wallis, *How Safe Are Our Skies?*, p. 112.

and Paris, where screening is mandatory. In addition, Air Canada has deployed screening equipment in areas deemed to be at increased risk, such as some Caribbean locations.¹⁶⁵⁹ Air Canada has not deployed X-ray equipment for cargo at Canadian airports mainly because it is not mandatory.¹⁶⁶⁰

The Commission heard that North America has lagged behind the rest of the world on cargo screening.¹⁶⁶¹ Other global airlines, such as Lufthansa¹⁶⁶² and Singapore Airlines, use X-ray technology to screen air cargo.¹⁶⁶³ The Commission was informed, for example, that Lufthansa uses a variety of methods to screen cargo, including X-ray and trace detection equipment and canine units. It also screens 100 per cent of air cargo leaving Germany for the United States. For shipments of air cargo to all other destinations, random screening occurs.¹⁶⁶⁴ Singapore Airlines uses X-ray equipment which can scan larger bulk cargo and also uses other methods, including canine units.¹⁶⁶⁵ In addition, equipment is currently being tested in Europe to enable an entire cargo pallet to be screened at once.¹⁶⁶⁶

In 1990 in the United States, the White House Commission on Aviation Safety and Security (Gore Commission) recommended using existing technologies and developing new ones for screening air cargo for explosives.¹⁶⁶⁷ In 2002, a review of air cargo security in the US revealed several technologies with the potential for enhancing security. They would be used for detecting explosives and other threat objects, including radiological, chemical and biological agents. These technologies and other methods for screening air cargo included:¹⁶⁶⁸

- Gamma-ray;
- Pulsed fast neutron analysis;
- Thermal neutron activation;
- X-ray, including bulk explosives detection systems (EDS);
- Radiation detection;
- Trace detection; and
- Vapour detection.

The Gore Commission report noted that these technologies all had security-enhancing benefits, but also potential limitations. The report suggested that

¹⁶⁵⁹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5259.

¹⁶⁶⁰ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5290.

¹⁶⁶¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5260; see also Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

¹⁶⁶² Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5253.

¹⁶⁶³ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4961.

¹⁶⁶⁴ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5252-5253.

¹⁶⁶⁵ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4961.

¹⁶⁶⁶ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5260; see also Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

¹⁶⁶⁷ Exhibit P-416, p. 12.

¹⁶⁶⁸ Exhibit P-416, p. 11.

existing trace explosives detection devices and bulk explosives detection systems used for screening passenger baggage could be used to screen cargo containers. The TSA reported that "...the use of trace devices to screen cargo has shown few problems."¹⁶⁶⁹ In 2005, TSA officials reported that the preliminary results of pilot testing programs about the applicability of EDS technology for individual pieces of air cargo ("break bulk cargo"), suggest that the technology was well suited for such use, although some limitations were identified. This technology's potential for screening air cargo was being assessed because it had already been used for inspecting checked baggage.¹⁶⁷⁰ In addition, electronic seals were recommended. These are radiofrequency devices that transmit an alarm when a container is compromised during transport or at cargo handling facilities.¹⁶⁷¹

Explosives Detection Dogs

The report made special mention of canines as one of the "most effective" and "most promising" methods for screening air cargo. The report noted that canine teams had "proven successful" and that their use had expanded significantly in the United States in recent years.¹⁶⁷² Sweet testified that canine units are particularly effective for screening large pallets of cargo. Canines can detect 5,000 to 7,000 different chemicals, organic compounds and other substances. Well-trained canines with good handlers are invaluable for air cargo screening. Sweet advised using canine units on a random basis or for individual risk assessments – for example, on a particular aircraft. She testified that the cost to train and maintain dogs was much less than the cost of purchasing and maintaining advanced technology.¹⁶⁷³

As with any method of screening, canine units have limitations. When used to detect explosives and other substances, dogs have limited attention spans. They can serve for roughly twenty minutes before they need a rest.¹⁶⁷⁴

Wallis agreed that canine units are very effective for screening air cargo and that they are usually used in specific circumstances. For example, in 1985, Air India requested bomb-detecting dogs to assist with screening checked baggage. Even at that time, Wallis testified, "...you had a carrier under high threat realizing the value of dogs."¹⁶⁷⁵

¹⁶⁶⁹ Exhibit P-416, p. 12.

¹⁶⁷⁰ Exhibit P-417, pp. 53-54.

¹⁶⁷¹ Exhibit P-416, p. 10 and footnote 4.

¹⁶⁷² Exhibit P-416, p. 12.

¹⁶⁷³ Sweet provided an estimate of the cost of training canine units as approximately \$10,000. See Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4954-4955. There was general consensus amongst witnesses that canine units are beneficial for screening cargo, although limitations were noted as discussed above. See also, for example, Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4247, Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5260, Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5006.

¹⁶⁷⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4955.

¹⁶⁷⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5006.

Working Toward a Cargo Screening Standard

Transport Canada cooperates with the United States on research, development, testing and evaluation of air cargo screening technologies.¹⁶⁷⁶ It appears that the United States is ahead of Canada in deploying these technologies. In 2005, the Government Accountability Office reported that, although a certification standard was being considered for air cargo inspection technologies, the TSA would permit air carriers to continue using the technologies and methods described in existing air carrier standard security programs and TSA security directives. These technologies and methods included the following: manual physical searches; X-ray systems; explosives trace detecting equipment; explosives detection systems; explosives detection canine teams; and decompression chambers.¹⁶⁷⁷

Cartwright testified that airlines in other countries may screen cargo using X-ray and other equipment. He suggested, however, that not all such screening would be sufficiently sophisticated to meet the requirements of Canadian regulations:

...It's that screening can mean different things. The fact that something is run through an imaging system, which, in the case of a large container, would be a higher energy X-ray usually or a gamma system, you can produce an image of it. That doesn't necessarily mean that you have the capacity or capability to detect the same criteria that we might establish, which we talked about as the standard, the standard being to be able to detect the same thing that you've required for detection for the standard passenger bag.

So without question, I think she [Sweet] is probably accurate in her statement that the screening is being done. The question is, is it being done at a level that is equivalent to what we have defined as being our baseline requirement?

He also questioned the quality of the equipment being used:

...And in some cases, certainly, some of the imaging systems are much like the imaging systems of old where they have no tools to assist the operator. And the question is, out of a very complex image, what level of success are you likely to have in identifying the kind of target materials and quantities that we have defined as being our baseline?¹⁶⁷⁸

¹⁶⁷⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5169.

¹⁶⁷⁷ Exhibit P-417, p. 53.

¹⁶⁷⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5213.

Duguay testified that equipment already in use for hold bag screening (HBS) could be used for cargo screening.¹⁶⁷⁹ Cartwright stated that technological developments in other areas of aviation security were applicable to some aspects of cargo security,¹⁶⁸⁰ but that not all screening equipment was suitable for all types of cargo.¹⁶⁸¹ Screening cargo is more complex than screening passengers or baggage because of its comparatively high variability. It is only in recent years that Transport Canada has engaged in research and development to assess air cargo screening technology.¹⁶⁸²

Whitaker testified that it was not possible to screen all cargo physically if the mechanisms to do so were not in place. He cited as an example the delays experienced in the US when it announced the move to 100 per cent cargo screening.¹⁶⁸³ He attributed the delays to the lack of necessary equipment. In contrast, Sweet stated that the delay in implementation had more to do with industry concerns about costs.¹⁶⁸⁴ Whitaker stated that, even though 100 per cent screening was not easy, it was "...certainly something that should be pursued quite aggressively."¹⁶⁸⁵

A further lesson of the Air India bombings is the danger of excessive reliance on poorly-developed technology. In 1985, the X-ray equipment deployed for baggage screening was in its infancy and, according to Wallis, was so rudimentary that its effect was simply cosmetic.¹⁶⁸⁶

In 1985, technology was used in place of both physical searches and passenger-baggage reconciliation – methods that were considered more effective but that were labour-intensive and time-consuming. Transport Canada itself appeared to encourage using technology for baggage screening because of the costs and inconvenience to airlines of slower, manual means of "matching and opening checked baggage."¹⁶⁸⁷

If Transport Canada holds a genuine belief, based on objective research, that a given technology for cargo screening does not meet the standard required, it is duty-bound not to deploy the technology until it meets that standard. However, Wallis wrote that good technology was well-established and already in place, at least by 2003.¹⁶⁸⁸ Cartwright appeared to concede that the technology is now available when he was asked about the estimated timeline for implementing screening technologies in Canada:

¹⁶⁷⁹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5260

¹⁶⁸⁰ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5131.

¹⁶⁸¹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5151.

¹⁶⁸² Exhibit P-188, p. 14.

¹⁶⁸³ Exhibit P-415.

¹⁶⁸⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4949.

¹⁶⁸⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4631.

¹⁶⁸⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4256-4257.

¹⁶⁸⁷ Exhibit P-101 CAF0581, p. 1.

¹⁶⁸⁸ Wallis, *How Safe Are Our Skies?*, p. 112.

There are technologies available today. The technology is evolving constantly.

Our goal and our challenge is to come up with enough of the technologies to be able to satisfy the requirements to be able to come up with a program. Will the program, five years from now, be the same as it is today? Probably not. But the whole purpose is to design it, as we did with the Hold Baggage Screening, is so that it can evolve and will get better as the technology comes along to help us.¹⁶⁸⁹

It is important to avoid excessive reliance on technology, but its judicious use serves as one important layer in the overall scheme of aviation security. Advanced systems already exist for passenger and baggage screening and have proven to be effective as part of a multi-layered approach to security. The anticipated increase in cargo volumes makes all the more important the assistance that X-ray and other technologies may offer.

Technology is constantly evolving. If good, reliable technology is currently available, it should be deployed (if necessary, with other measures to compensate for any limitations of the technology) as one layer in the process of securing air cargo. Given the security risks posed by air cargo, Canada cannot afford to wait.

Interim Measures

Even if Transport Canada concludes that appropriate equipment for searching cargo does not yet exist, this does not absolve the Department of the responsibility to ensure that cargo is secure. Alternatives to technology must be used.

Air Canada does precisely this for a certain segment of air cargo. Air Canada is required to screen “non-exempt”¹⁶⁹⁰ cargo moving out of Montreal, Toronto and Vancouver destined for the United States.¹⁶⁹¹ Duguay explained that, though Air Canada did not have access to technical equipment to screen cargo, screening alternatives were available. One was a manual search. Guards have been hired at Air Canada’s three major centres – Vancouver, Toronto and Montreal – expressly to search US-bound non-exempt cargo manually.¹⁶⁹² Duguay testified that Air Canada exceeds the US requirement by screening 100 per cent of non-exempt cargo shipped to the US.¹⁶⁹³

¹⁶⁸⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5207.

¹⁶⁹⁰ There are a number of criteria that enable cargo to be classified as “exempt” from the screening requirement. These are specified in the Canadian regulations as well as in the Model Security Program of the Transport Security Administration (TSA), which the United States provides to foreign carriers such as Air Canada. One criterion, for example, is designation as a certified shipper. See Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5252, 5254.

¹⁶⁹¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5253-5254.

¹⁶⁹² Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5290.

¹⁶⁹³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5253.

Clearly, it is possible to search at least a portion of air cargo before it is loaded onto an aircraft. Where a requirement to do this has existed, air carriers have complied. Duguay testified that the measures used for searching non-exempt cargo could be applied to exempt cargo as well, based on risk and threat analysis.¹⁶⁹⁴

Interim measures have been part of the screening program in the United States while it awaits more advanced technology. TSA officials reported that, in the absence of formally approved technology, air carriers will be permitted to continue to use existing technologies and methods that are described in air carrier standard security programs and TSA security directives. These measures include manual physical searches, X-ray equipment, EDT equipment, explosive detection systems and canine teams.¹⁶⁹⁵

The air cargo industry operates with time-sensitive cargo.¹⁶⁹⁶ That cargo represents a significant source of revenue for airlines,¹⁶⁹⁷ and many in the industry maintain that time constraints and the volume of cargo present a challenge for screening at airports.¹⁶⁹⁸ Yet air carriers seem able to comply with screening obligations in jurisdictions where cargo searches are required – for example, in Canada for non-exempt cargo headed to the US. Impediments to searching all air cargo in Canada may flow more from concerns about ease, convenience and expense than from valid concerns about the cargo's time sensitivity or volume.

3.8.1.3.5 Inadequate Training

However searches of cargo are performed, they are of little use if done poorly. Sweet testified that insufficient training of cargo handlers has resulted in poor search techniques and a lack of security awareness. She stressed that cargo loaders and cargo screeners need to better understand their tasks. Cargo handlers must know what they are looking for in cargo, and they also need to better appreciate the impact on aircraft security. She gave examples of cursory physical searches, such as not removing shrink-wrap from cargo because of the perceived difficulty of doing so, or inspecting only one box of a large pallet. Sweet stated that such practices provide no assurance that cargo is secure.¹⁶⁹⁹ Along with training, supervision and monitoring of cargo handlers are also important.

Deficiencies in training worsen an already distressing situation. Following the loss of Air India Flight 182, new training programs for screeners were developed, but these appear to have been restricted to passenger screening.¹⁷⁰⁰ This is consistent with the fact that passengers and baggage were the main priority

¹⁶⁹⁴ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5292.

¹⁶⁹⁵ Exhibit P-417, p. 53.

¹⁶⁹⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5203.

¹⁶⁹⁷ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4246.

¹⁶⁹⁸ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5187.

¹⁶⁹⁹ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4953-4954.

¹⁷⁰⁰ Exhibit P-263, pp. 68, 70.

at the time. The evidence showed that it was not until 2001, in the wake of the events of September 11th, that cargo training programs began to be addressed. In October of that year, the Government announced an initiative to fund training programs for cargo handlers to support the implementation of new technologies.¹⁷⁰¹

Training for air cargo security in Canada continues to focus on screening, the process applied when cargo is presented for acceptance by a carrier. In 2003, Transport Canada revised its screening training for all employees involved in cargo acceptance at Class 1 and Class 2 airports. The aim was to give the employees the knowledge and skills needed to perform their duties as air cargo screeners.¹⁷⁰² However, no mention was made of any training for the actual physical search of air cargo. Screening, as Duguay explained, is the process that occurs when a shipper tries to get cargo accepted by a carrier's agent, who considers the description of the merchandise, whether the shipper is familiar, and other factors. Searching involves actually examining the cargo.¹⁷⁰³

There appears to be very little training about searching cargo in Canada. As previously discussed, the Commission was told that all Air Canada's non-exempt cargo transported to the United States is physically searched by guards.¹⁷⁰⁴ The Commission was also advised that air carriers may choose to search cargo in certain circumstances.¹⁷⁰⁵ The absence of training, however, provides little comfort that the searches are performed properly. As Sweet testified, poorly executed searches are no searches at all.¹⁷⁰⁶

Sweet spoke highly of the UK training system relating to cargo. Training is required for any person handling cargo and consists of a two-day initial training session and an annual refresher course. She emphasized that "anybody touching cargo [by] any means whatsoever" must take the training.¹⁷⁰⁷

3.8.1.3.6 Poor Access Control

Sweet testified that access to air cargo is also not well controlled in the US and spoke about inadequate non-passenger screening (NPS). She testified that too many people, whose job functions do not intersect with cargo activities and who may not have been security-screened or subjected to background clearances, nonetheless have access to cargo.¹⁷⁰⁸

In 2005, the US Government Accountability Office drew attention to the security risks posed by air cargo because of inadequate background investigations of those handling cargo and the illegal shipment of hazardous materials. Cargo

¹⁷⁰¹ Exhibit P-157, p. 98 of 135.

¹⁷⁰² Exhibit P-263, p. 86.

¹⁷⁰³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5254.

¹⁷⁰⁴ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5290.

¹⁷⁰⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4651.

¹⁷⁰⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4954.

¹⁷⁰⁷ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4958.

¹⁷⁰⁸ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4945-4946.

theft was seen as an indication of potential weaknesses in air cargo security.¹⁷⁰⁹ Similar concerns exist in Canada. In 2007, the Senate Committee reported its dismay at the potential connection between organized crime at airports and airport security. Describing airports as “riddled” with organized crime, the Committee observed that criminals were profiting from gaps in security. Those same gaps could help terrorists.

The Committee also concluded that the interests of some organized crime groups overlap with those of terrorists. Among the solutions proposed by the Committee were addressing concerns surrounding insufficient policing, inadequate background checks and inadequate control of access to restricted areas.¹⁷¹⁰

3.8.1.3.7 Enhancements Required

The eighth edition of Annex 17, issued in 2006, requires security controls for cargo and mail:

4.6.4 Each Contracting State shall ensure that operators do not accept cargo or mail for carriage on an aircraft engaged in passenger commercial air transport operations unless the application of security controls is confirmed and accounted for by a regulated agent, or such consignments are subjected to appropriate security controls.

Canada does not appear to meet its obligations even under what is acknowledged to be merely a minimum standard. It has no regulated agent program, nor are appropriate security controls applied to air cargo.

3.8.1.4 Proposal for an Enhanced Regime: Air Cargo Security Initiative

Only within the last five years has the Government of Canada publicly acknowledged that air cargo security is wanting. In April 2004, it unveiled its first National Security Policy, which identified enhanced air cargo security as a priority.¹⁷¹¹

Following this declaration, Transport Canada began to evaluate existing security requirements for air cargo.¹⁷¹² It held consultations with industry stakeholders, assessed air cargo security in other jurisdictions, considered technological advances and conducted an air cargo risk assessment. As a result, the Department

¹⁷⁰⁹ It was reported that cargo theft in the United States is estimated to range in the billions of dollars annually. See Exhibit P-417, p. 24.

¹⁷¹⁰ Exhibit P-172, pp. 17-18 of 155.

¹⁷¹¹ Exhibit P-418, p. 38.

¹⁷¹² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5183.

recommended advancing to the next phase of the initiative – program design and pilot testing.¹⁷¹³

In the federal Budget of 2006, the Government allocated \$26 million over two years to support design and pilot testing.¹⁷¹⁴ These funds were to assist with two principal aspects of air cargo security: "...the development of measures to ensure cargo security throughout the supply chain, as well as the evaluation of screening technologies."¹⁷¹⁵ The Air Cargo Security (ACS) Initiative was launched as a result,¹⁷¹⁶ led by Transport Canada and supported by the Canada Border Services Agency (CBSA).¹⁷¹⁷ The Initiative's purpose was "...to address the continuing threat of terrorism, escalating international aviation security standards and Canadian security needs."¹⁷¹⁸ The CATSA Advisory Panel stated that this infusion of funding demonstrated Canada's commitment to take action on air cargo security and to honour the promise contained in the 2004 National Security Policy.¹⁷¹⁹

However, others have been discouraged by an apparent lack of progress. In its 2007 follow-up report on aviation security, the Senate Committee noted that air cargo security was "... still at the discussion stage more than five years after 9/11...."¹⁷²⁰

The Senate Committee was also discouraged by Transport Canada's apparent attention to competing economic interests. In its July 7, 2006, response to the Senate Committee's 2003 report on aviation security, Transport Canada referred to policy discussions with stakeholders that started in 2004. The Committee, responding in its own 2006 report, stated that emphasis was placed on facilitating the "efficient movement of goods,"¹⁷²¹ and that consultations with stakeholders amounted to discussions with those having a financial stake in air transport. The Committee recognized that economic and efficiency interests are a reality of the air cargo industry, but suggested that such interests may impede air cargo security. The Committee cautioned that efficiency measures should not "trump" security measures.¹⁷²²

The Senate Committee was nonetheless encouraged that Transport Canada had at last openly acknowledged deficiencies in air cargo security. Although the Committee felt that Transport Canada had hitherto considered its views "alarmist," the Committee praised the Department in its 2007 report for finally putting "...the Government of Canada firmly on record as acknowledging the existence of 'the air cargo security gap' – a gap the Committee has been pointing

¹⁷¹³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5183; see also Exhibit P-172, pp. 41-42 of 155.

¹⁷¹⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5183.

¹⁷¹⁵ Exhibit P-169, p. 54 of 202.

¹⁷¹⁶ Exhibit P-419.

¹⁷¹⁷ Final Submissions of the Attorney General of Canada, Vol. II, para. 354.

¹⁷¹⁸ Exhibit P-419.

¹⁷¹⁹ Exhibit P-169, p. 54 of 202.

¹⁷²⁰ Exhibit P-172, pp. 66-67 of 155.

¹⁷²¹ Exhibit P-172, pp. 42-43 of 155.

¹⁷²² Exhibit P-172, p. 42 of 155.

to for five years now.”¹⁷²³ In testimony before the Senate Committee on June 19, 2006, Louis Ranger, Deputy Minister at Transport Canada, also conceded as much when questioned about the new initiative for cargo security, stating, “We have been concerned. There are gaps there that we need to deal with.”¹⁷²⁴

The ACS Initiative proposed a major overhaul of the air cargo security regime, the first ever undertaken in Canada. In accordance with the 2006 federal Budget directive, Transport Canada adopted a “two-pronged approach” to improving air cargo security: hardening supply chain security and improving cargo screening. The first involved establishing a national system of regulated agents to ensure that air cargo was secure from its point of origin to its arrival at an aircraft. Air cargo that was secured in this way was considered low risk, which was the primary goal of hardening supply chain security. The second prong of the approach involved assessing and developing screening technologies and protocols for air cargo, with an emphasis on high risk or “targeted” cargo.¹⁷²⁵

These developments coincided roughly with the first detailed audit of Canada’s aviation security regime, conducted by ICAO in the spring of 2005.

3.8.1.4.1 Developments in Air Cargo Security in the United States

The development of the proposed ACS Initiative in Canada coincided with air cargo security developments in the United States.¹⁷²⁶ There, the security of air cargo is the responsibility of the TSA, created in November 2001 by the *Aviation and Transportation Security Act*.¹⁷²⁷ Until recently, the emphasis of air cargo security was on passenger aircraft.¹⁷²⁸ Air carriers and freight forwarders were required to have TSA-approved security programs in order to ship cargo on passenger aircraft.¹⁷²⁹ In 2001, the Act required that all cargo carried on board passenger aircraft be screened and that a system for screening, inspecting or otherwise ensuring the security of cargo on all-cargo aircraft be established “as soon as practicable.”¹⁷³⁰ In May 2006, new air cargo regulations were issued to improve the security of air cargo, in part by extending many of the security requirements for passenger aircraft to all-cargo aircraft. These measures stemmed from the two risks seen by the US as paramount in air cargo – the use

¹⁷²³ Exhibit P-172, p. 41 of 155.

¹⁷²⁴ Exhibit P-172, p. 66 of 155.

¹⁷²⁵ Final Submissions of the Attorney General of Canada, Vol. II, paras. 354-356.

¹⁷²⁶ Information respecting air cargo security in the United States is largely limited to documentary evidence that derives mainly from publicly available government reports. The Commission’s hearings did not focus in any extensive manner on aviation security in the United States. However, the Commission felt that the information contained in some publicly available documents provided a useful basis for comparison in air cargo security.

¹⁷²⁷ Exhibit P-416, p. 1.

¹⁷²⁸ Exhibit P-416, p. 1.

¹⁷²⁹ Exhibit P-416, p. 8.

¹⁷³⁰ Exhibit P-416, p. 1. The terms “screen” and “inspect” are understood in the same manner as their Canadian counterparts. Screening refers to the “...systematic evaluation of a person or property to assess whether either poses a threat to security.” Inspection is a method of conducting such an evaluation, but is not the only method. The TSA considers inspection to be a subset of screening. See Exhibit P-415, p. 30484.

of cargo to introduce an explosive device on board passenger aircraft, and the takeover of an all-cargo aircraft and its use as a weapon.¹⁷³¹

In 2002, the US General Accounting Office (GAO), the predecessor to the Government Accountability Office, released a report that described the susceptibility of air cargo to sabotage. The report observed that "...[i]f vulnerabilities exist in the transport of air cargo, they potentially threaten the air transport system."¹⁷³² It noted that vulnerabilities in air cargo security had been identified as early as 1996 by the Gore Commission, and by a number of other government and industry studies. It cited weaknesses in air carrier and freight forwarder security procedures, including inadequate background checks for cargo handlers, and problems with cargo tampering.¹⁷³³

As in Canada, the GAO report found that aviation security efforts in the US had focused almost entirely on improving passenger and baggage security, leaving air cargo exposed. The report noted that, despite the legislative requirement to screen all cargo travelling on passenger aircraft, only a limited amount was being screened. This was attributed to the large volume of cargo and the fact that cargo delivery was considered time-critical.¹⁷³⁴

The report noted that the TSA, like the FAA before it, had been slow to move on numerous recommendations of the Gore Commission and other industry studies. Like the Gore Commission, the GAO report stressed the need for a comprehensive security plan outlining long-term goals, performance targets, time frames for completing security improvements and risk-based criteria to prioritize actions for achieving those objectives. It also recommended incorporating a risk management approach into air cargo security to assist in systematically evaluating and prioritizing various technological and operational security improvements.¹⁷³⁵

In January 2003, the TSA formed a working group with industry stakeholders to address air cargo security. Of note, the working group involved family members of the victims of Pan Am Flight 103, as well as groups representing airlines, pilots, freight forwarders and government agencies.¹⁷³⁶ In November 2003, the TSA issued an Air Cargo Strategic Plan that outlined a layered, threat-based and risk-managed approach to air cargo security.¹⁷³⁷ The plan focused on the perceived risks of explosive devices on passenger aircraft and of the hijacking of all-cargo aircraft. As part of its risk-management approach, the plan highlighted four strategic objectives:¹⁷³⁸

¹⁷³¹ Exhibit P-415, p. 30479.

¹⁷³² Exhibit P-416, p. 1.

¹⁷³³ Exhibit P-416, p. 8.

¹⁷³⁴ Exhibit P-416, p. 20.

¹⁷³⁵ Exhibit P-416, pp. 20-21.

¹⁷³⁶ Exhibit P-417, pp. 17, 77.

¹⁷³⁷ Exhibit P-415, p. 30479; see also Exhibit P-417, pp. 17-18.

¹⁷³⁸ Exhibit P-417, pp.4-5.

1. Enhancing cargo shipper and cargo supply chain security;
2. Identifying elevated risk cargo through pre-screening and ensuring that 100 per cent of such cargo is inspected;
3. Identifying technology for inspecting elevated risk cargo; and
4. Strengthening the security of all-cargo aircraft and cargo operation areas.

The GAO concluded that the air cargo strategic objectives tied into the broader aviation and homeland security objectives contained in TSA's agency-wide strategic plan for transportation. They also reflected the goals of the strategic plan of the DHS, of which the TSA is a part.¹⁷³⁹

The Government of Canada announced its own National Security Plan in April 2004, naming air cargo security as a priority.¹⁷⁴⁰ However, Transport Canada still does not have a written national civil aviation security program, as required by Annex 17.¹⁷⁴¹ With the proposal in Canada for a new initiative in air cargo security, a clear, written national security program can ensure harmonization and consistency within the overall aviation security regime.

In November 2004, the TSA published a notice of proposed rulemaking (NPRM) to solicit public comment on proposed air cargo security regulations. As outlined in the TSA's Air Cargo Strategic Plan, the NPRM recommended adopting a threat- and risk-based approach to air cargo security and focusing the TSA's efforts on the two critical risks described above – the use of cargo to introduce an explosive device on passenger aircraft, and the takeover of an all-cargo aircraft and its use as a weapon. The NPRM also proposed creating a new security regime for all-cargo aircraft that met a minimum weight requirement, requiring enhanced security controls on access to cargo and improving security requirements for indirect air carriers,¹⁷⁴² the term given to regulated agents in the United States.¹⁷⁴³

On May 26, 2006, the DHS issued its Final Rule on Air Cargo Security Requirements (Final Rule), which adopted the regulatory amendments proposed in the NPRM, with only minor revisions.¹⁷⁴⁴ This marked the first substantial amendments to air cargo regulations in the United States since 1999.¹⁷⁴⁵ In addition to general enhancements to air cargo security, the Final Rule sought to extend to all-cargo aircraft many of the air cargo security procedures that then applied to passenger aircraft.¹⁷⁴⁶

¹⁷³⁹ Exhibit P-417, p. 18

¹⁷⁴⁰ Exhibit P-418, p. 38.

¹⁷⁴¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5017-5018.

¹⁷⁴² Exhibit P-415, p. 30479.

¹⁷⁴³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5192.

¹⁷⁴⁴ Exhibit P-415, p. 30478.

¹⁷⁴⁵ Exhibit P-421.

¹⁷⁴⁶ Exhibit P-415, p. 30496.

Some of the general air cargo security enhancements provided by the Final Rule included:

- Improved background security checks of individuals working for air carriers and indirect air carriers;¹⁷⁴⁷
- Extension of designated areas of airports where security controls apply to protect cargo;¹⁷⁴⁸
- Extension of the TSA's inspection authority of air carriers to include off-airport locations or areas operated by an agent in furtherance of an air carrier's security responsibilities;
- Enhanced provisions for screening and accepting cargo by foreign air carriers;¹⁷⁴⁹
- Strengthened requirements for air cargo acceptance;¹⁷⁵⁰
- Criminal background checks for cargo screeners who do not already possess identification for sterile areas;
- Codification of the "known shipper" program;¹⁷⁵¹
- Consolidation of private industry "known shipper" lists into one central "known shipper" database managed by the TSA;¹⁷⁵²
- Extension of security requirements to agents of indirect air carriers;¹⁷⁵³ and
- Enhanced training for indirect air carrier employees and agents.¹⁷⁵⁴

Some amendments were consistent with expanding security functions to persons and property on all-cargo aircraft. They included:

- Security programs for all-cargo aircraft that meet a minimum weight requirement,¹⁷⁵⁵ certain foreign all-cargo air carriers¹⁷⁵⁶ and indirect air carriers providing cargo to all-cargo aircraft;¹⁷⁵⁷
- Prohibition of the carriage of weapons, explosives and incendiaries by individuals;¹⁷⁵⁸ and
- Prevention of unauthorized access to the operational area of the aircraft while loading and unloading cargo.¹⁷⁵⁹

¹⁷⁴⁷ Exhibit P-415, p. 30496.

¹⁷⁴⁸ Exhibit P-415, p. 30497.

¹⁷⁴⁹ Exhibit P-415, p. 30499.

¹⁷⁵⁰ Exhibit P-415, p. 30498.

¹⁷⁵¹ Exhibit P-415, p. 30499.

¹⁷⁵² Exhibit P-421, p. 1.

¹⁷⁵³ Exhibit P-415, p. 30500.

¹⁷⁵⁴ Exhibit P-415, p. 30501.

¹⁷⁵⁵ Exhibit P-415, p. 30499.

¹⁷⁵⁶ Exhibit P-415, p. 30479.

¹⁷⁵⁷ Exhibit P-415, p. 30500.

¹⁷⁵⁸ Exhibit P-415, p. 30496.

¹⁷⁵⁹ Exhibit P-415, p. 30498.

In addition, since November 2003, TSA security directives required aircraft operators and foreign air carriers to inspect a portion of their air cargo. The NPRM proposed codifying the inspection requirement. Legislation passed in 2005 tripled the percentage of cargo that had to be inspected.¹⁷⁶⁰ In August 2007, legislation was enacted to require 100 per cent screening of air cargo transported on passenger aircraft by 2010.¹⁷⁶¹

The changes proposed to air cargo security in Canada echo many of the changes taking place, or that have already taken place, in the United States. Captain Craig Hall, Director of the National Security Committee of ALPA, observed that "...[m]uch of what we do in cargo screening is driven by our friends to the south, because in many respects our system is going to have to mirror theirs...." He stated that the US is Canada's largest trade partner and that Canada's system will need to meet US standards.¹⁷⁶²

Harmonization and interoperability will always be important, but slow movement on a security issue in the US must not be allowed to dictate progress in Canada. The United Kingdom did not wait for others in the European or international community before it introduced its comprehensive regulated agent program in 1993. The program became a model for others, including Canada. After the release of the Seaborn Report in 1985, Canada did not wait for other countries before introducing passenger-baggage reconciliation.¹⁷⁶³

Programs to address threats can be modified, if necessary, as other countries come on board. In any event, as Cartwright acknowledged, cargo screening programs can never be static. Newer and better technologies will continuously appear, but this must not stall implementation of security measures before then. The best available security procedures should be put in place, using a layered approach to minimize weaknesses.

3.8.1.4.2 Hardening Supply Chain Security

To harden supply chain security, Transport Canada is focusing on two projects. The first seeks to establish a system of regulated agents to secure low risk air cargo throughout the supply chain.¹⁷⁶⁴ Transport Canada proposes a three-tiered system of regulated entities that will ultimately involve all levels of the supply chain – shippers, freight forwarders and air carriers.¹⁷⁶⁵ All regulated entities will be required to apply security measures to air cargo, as specified by Transport Canada.¹⁷⁶⁶

¹⁷⁶⁰ Exhibit P-415, p. 30479.

¹⁷⁶¹ Exhibit P-422, pp. 9-10.

¹⁷⁶² Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8009.

¹⁷⁶³ Exhibit P-157, p. 66 of 135.

¹⁷⁶⁴ Exhibit P-422, p. 5; see also Final Submissions of the Attorney General of Canada, Vol. II, para. 355.

¹⁷⁶⁵ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁷⁶⁶ Exhibit P-419.

The second project aims to support the supply chain security programs through a database, known as the Secure Supply Chain Management System (SSCMS). The SSCMS will act as a central repository of industry information and provide a portal for industry and government to share information. According to Transport Canada, data entered into this system will be validated against other sources¹⁷⁶⁷ and will help government identify secure partners and effectively manage program participation.¹⁷⁶⁸ Transport Canada plans to evaluate the interoperability of the SSCMS with various national and international supply chain security initiatives, including the US Known Shipper Management System.¹⁷⁶⁹

The Known Shipper database was established in the United States in 2002¹⁷⁷⁰ to streamline the process by which shippers, both individuals and businesses, are made known to the air carriers with whom they conduct business. In its 2005 report on air cargo security, the US GAO identified factors that may have limited the effectiveness of this system. In particular, information in the database was incomplete and potentially unreliable because participation in the database was voluntary. The report also stated that the TSA had not taken steps to identify shippers which may pose a security threat.¹⁷⁷¹ Mandatory Known Shipper registration, which came into effect with the 2006 Final Rule on Air Cargo Security Requirements, was expected to rectify some problems. Concerns similar to those identified with the US system may arise as Canada develops the SSCMS.

Supply Chain Security Program

Under the Canadian supply chain security program, each regulated entity will be required to apply security procedures to air cargo at their facilities and during transport, and to maintain the integrity of secure cargo at all points of transfer.¹⁷⁷² By applying appropriate security processes to cargo before its arrival at the airport, regulated agent programs in effect extend the perimeter of the airport.¹⁷⁷³ Stephen Conrad, Transport Canada's Project Director for Air Cargo Security, testified that it is not practical in most industrialized nations to wait to secure all cargo when it reaches the airport. Most large centres receive large volumes of cargo and face time, space and capacity constraints. A bottleneck is inevitably created, which can lead to unacceptable delays for time-sensitive cargo.¹⁷⁷⁴ By redirecting some responsibility for securing air cargo to earlier points in the supply chain, bottlenecks at the airport can be greatly reduced.¹⁷⁷⁵

¹⁷⁶⁷ Exhibit P-419.

¹⁷⁶⁸ Final Submissions of the Attorney General of Canada, Vol. II, para. 355.

¹⁷⁶⁹ Exhibit P-419.

¹⁷⁷⁰ Exhibit P-417, p. 76.

¹⁷⁷¹ Exhibit P-417, p. 5.

¹⁷⁷² Exhibit P-419.

¹⁷⁷³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5185.

¹⁷⁷⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5187.

¹⁷⁷⁵ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5190.

The aim is to have a full, nationwide, regulatory framework in place,¹⁷⁷⁶ with Transport Canada providing oversight and compliance monitoring, either directly or through a delegate.¹⁷⁷⁷ Participating shippers, freight forwarders and air carriers will be required to have security plans and to maintain secure premises and practices accordingly.¹⁷⁷⁸ All participating shippers, freight forwarders and air carriers will be certified by Transport Canada¹⁷⁷⁹ and will be known, respectively, as “Regulated Shippers,” “Regulated Agents” and “Regulated Air Carriers.” Regulated entities will be subject to inspection by Transport Canada Security Inspectors or by a combination of inspectors and a government-licensed or government-certified body.¹⁷⁸⁰

Shippers represent the most distant point in the supply chain. They are the originators of cargo and consist of manufacturers and exporters who prepare cargo for shipment.¹⁷⁸¹ Shippers participating in the program will be required to “validate,” upon packaging, that the cargo does not contain anything harmful to civil aviation.¹⁷⁸² At the point of transfer to another entity in the supply chain, such as a participating freight forwarder or air carrier, shippers will be required to certify that 100 per cent of their cargo has been screened or inspected. Alternatively, shippers must identify cargo that requires inspection or screening.¹⁷⁸³

Freight forwarders are intermediaries, performing functions such as cargo storage, consolidation and transport.¹⁷⁸⁴ Air carriers are the final recipients of cargo before its air transport. Participating freight forwarders and air carriers must verify that cargo is secure when they accept it from another entity in the supply chain. If they detect a breach in security, they must have the capacity to screen or inspect cargo.¹⁷⁸⁵

At every point of transfer in the supply chain, there will be a formal process of certification that the cargo being transferred is secure, as well as verification that the cargo being accepted has remained secure. At each point of transfer, each regulated entity must answer one question: “Is the cargo secure?”¹⁷⁸⁶ Using this process, the cargo can be secured as far back as the shipper and the point of packaging.¹⁷⁸⁷

Conrad testified that very few countries have regulated agent programs that include shippers.¹⁷⁸⁸ He stated that Transport Canada believes that establishing

¹⁷⁷⁶ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5200.

¹⁷⁷⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5200.

¹⁷⁷⁸ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁷⁷⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5190.

¹⁷⁸⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5200.

¹⁷⁸¹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁷⁸² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁷⁸³ Exhibit P-189, p. 6; see also Exhibit P-101 CAF0827, p. 3.

¹⁷⁸⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189; see also Exhibit P-189, p. 7.

¹⁷⁸⁵ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁷⁸⁶ Exhibit P-189, p. 7.

¹⁷⁸⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5190.

¹⁷⁸⁸ Exhibit P-101 CAF0872, p. 4.

a full regulatory framework for shippers constitutes a further step that will “close the loop” on the entire supply chain.¹⁷⁸⁹ The Commission agrees that full regulation of all levels of the supply chain is desirable.

As under the current legislation, air carriers in the proposed supply chain security program will retain primary responsibility for screening air cargo, in the broadest sense of the term “screening.”¹⁷⁹⁰ The program recognizes that air carriers may have a limited ability to screen or search cargo. For example, an air carrier may not have appropriate equipment, the capacity to screen certain types of cargo or the ability to perform particular security functions. Whatever the reason, if an air carrier is not confident that cargo is secure, the cargo must not travel on an aircraft.¹⁷⁹¹

As an added layer of security, air cargo at every level of the supply chain will also be subject to random secondary screening and inspection.¹⁷⁹² In sum, supply chain security for air cargo consists of a series of validation, certification and verification processes performed by regulated entities, with additional screening and inspection measures superimposed on a random and targeted basis.

As is the case for many of the security measures under the US Final Rule, the regulated supply chain security system applies to air cargo destined for passenger aircraft and all-cargo aircraft. Also like the US program, the focus of screening and inspection measures in Canada will differ for all-cargo aircraft, because the perceived primary risks are different from those of passenger aircraft. Where cargo is to be transported on passenger aircraft, screening and inspection procedures will aim at detecting and preventing the introduction of explosive devices. Where cargo is to be carried on all-cargo aircraft, screening and inspection will be directed at detecting and preventing stowaways from commandeering the aircraft.¹⁷⁹³ Cargo that is transferred from all-cargo aircraft to passenger aircraft will require additional screening or inspection.¹⁷⁹⁴

The 2005 report of the US GAO noted that industry stakeholders criticized the dual focus of air cargo security in the United States – that of preventing the introduction of explosive devices on passenger aircraft and the hijacking of all-cargo aircraft. The criticism was that the focus did not fully address the potential risks posed by air cargo.¹⁷⁹⁵ Experts and stakeholders spoke of the need to address a third threat – placing an explosive device containing a weapon of mass destruction on an all-cargo aircraft. TSA officials stated that the TSA decided to focus only on two threats because these were the most likely scenarios, though it would nonetheless address any potential new threats as needed. In fact, the TSA stated that it had identified and was reviewing a new, emerging threat to

¹⁷⁸⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5196.

¹⁷⁹⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5188.

¹⁷⁹¹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5195.

¹⁷⁹² Exhibit P-422, pp. 6-8.

¹⁷⁹³ Exhibit P-422, p. 8.

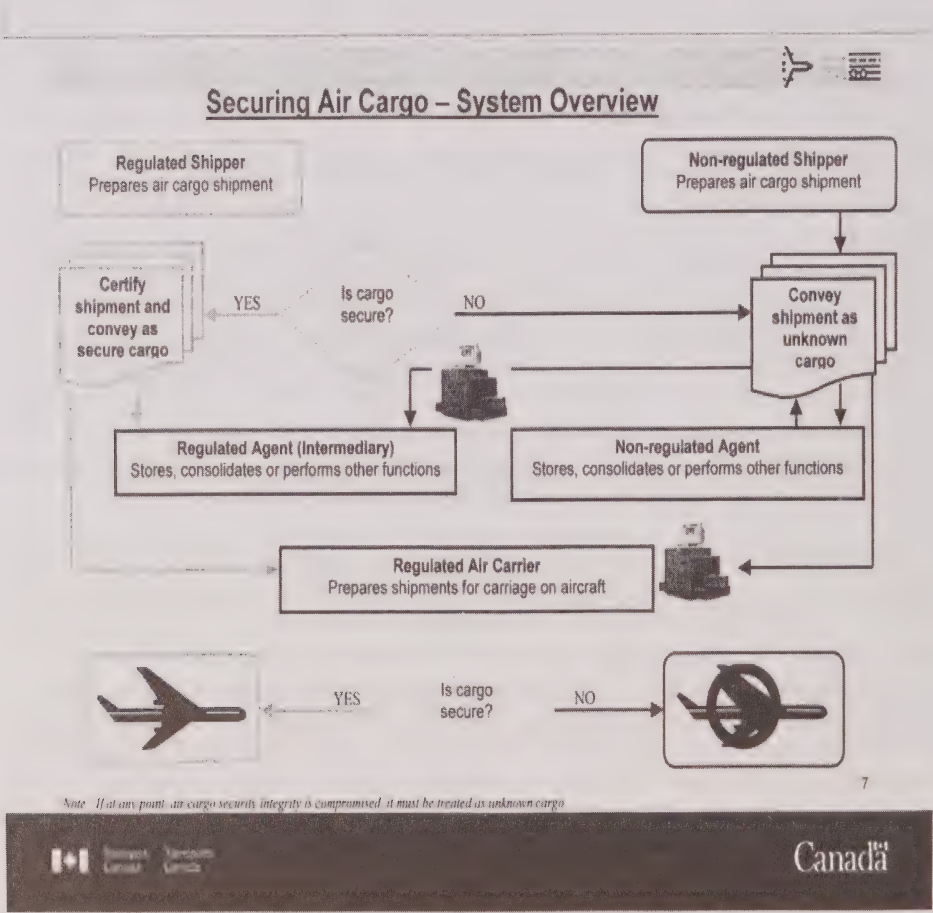
¹⁷⁹⁴ Exhibit P-422, p. 8.

¹⁷⁹⁵ Exhibit P-417, p. 4.

air cargo on passenger aircraft at the time of its 2005 report. Information about the threat was “security sensitive” and not disclosed.¹⁷⁹⁶

The Commission agrees that the security focus on stowaways in all-cargo aircraft may fail to address the additional risk of explosives being placed on such aircraft. As previously noted, there is disagreement about the degree of risk that all-cargo aircraft pose in Canada.¹⁷⁹⁷ Transport Canada needs to offer further justification for focusing only on stowaways.

Figure 1
Supply Chain Security System
Exhibit P-189, p. 7



¹⁷⁹⁶ Exhibit P-417, pp. 20-21 and footnote 38.

¹⁷⁹⁷ Exhibit P-169, p. 53 of 202; Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4683.

Although all commercial air carriers remain subject to formal regulation for air cargo security, the supply chain security program will not be mandatory for all shippers and freight forwarders in Canada. Conrad provided two reasons for this: cost to industry and procedural challenges. Under the supply chain security program, regulated entities and Transport Canada will pay their own operating costs.¹⁷⁹⁸ For some private companies dealing with low volumes of air cargo, the costs could be significant for them and, in some cases, prohibitive.¹⁷⁹⁹ Conrad described the experience of the United States in attempting to fully regulate all shippers and freight forwarders. There were difficulties implementing the program due to the vast number of shippers and the challenges of monitoring the security status of such a large group.¹⁸⁰⁰

Instead, in Canada, a parallel system of non-regulated shippers and freight forwarders will operate alongside the supply chain security program. All cargo originating from non-regulated shippers or freight forwarders will be considered high risk and will be subject to various screening and inspection methods.¹⁸⁰¹ Non-regulated shippers will fall into one of three categories: Unknown Shippers (those not known to freight forwarders or air carriers in the supply chain program); Known Shippers (those that are “known” to freight forwarders or air carriers, as that term is defined in the confidential regulations and measures); and Registered Shippers (those “...vetted by an approved process and recognized nationally”).¹⁸⁰² Cargo originating from Unknown or Known Shippers will face additional restrictions if destined for US passenger aircraft.¹⁸⁰³ Cargo received from Non-Regulated Agents will be placed in the same sort of unknown, known and registered categories.

There will still be many instances where cargo arrives directly at the airport and requires full security controls. For example, individuals may appear at the airport to ship a package. The counter services at the airport offered by many airlines work well for this segment of cargo. Conrad advised that the need to secure cargo at the airport will continue and that the capacity to do so must be maintained. One advantage of securing cargo at the airport is the elimination of vulnerabilities further out in the supply chain. However, as noted earlier, it would not be feasible to screen all air cargo at the airport, particularly in large cities.¹⁸⁰⁴

As part of the pilot testing and development phase, Transport Canada introduced the freight forwarder community to the Regulated Agent Program in June 2007. Since then, about 120 freight forwarders have indicated their interest in

¹⁷⁹⁸ Exhibit P-423, p. 11.

¹⁷⁹⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5193-5194. Conrad indicated that studies have shown that the costs of infrastructure and security process modifications required to comply with some supply chain systems have ranged between \$20,000 and \$250,000.

¹⁸⁰⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5190.

¹⁸⁰¹ Exhibit P-422, p. 6.

¹⁸⁰² Exhibit P-422, p. 6.

¹⁸⁰³ Exhibit P-422, p. 6.

¹⁸⁰⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5187-5188.

participating and are at various stages of enrolment.¹⁸⁰⁵ The Regulated Agent Program was formally launched in June 2008.¹⁸⁰⁶

Oversight and Compliance Monitoring

Key to the hardening of supply chain security is the requirement that every participating entity, at each level of the cargo supply chain, draft and maintain a security plan detailing its security measures.¹⁸⁰⁷ During the development phase of the supply chain security program, MOUs will establish guidelines so that Regulated Shippers and Regulated Agents can meet this requirement. Transport Canada has indicated that, when the program is fully implemented, this requirement will be subject to “possible” formal regulation under the *Aeronautics Act* for Regulated Shippers and “likely” formal regulation for Regulated Agents. Air carriers are already obliged to maintain security plans under the *Air Carrier Security Measures*, although enhancements to the Measures are possible as the program develops, with regulatory amendments to the *Aeronautics Act* expected at full implementation of the supply chain security program.¹⁸⁰⁸

MOUs are already being implemented as part of the Regulated Agent Program launched in 2008.¹⁸⁰⁹ The MOUs describe the respective responsibilities of Transport Canada and Regulated Agents, and focus mainly on the mandatory security plans. Under the MOUs, the freight forwarder is responsible for submitting to Transport Canada specific Air Cargo Security Plans for each of its facilities. The plans must include required elements as outlined by Transport Canada.¹⁸¹⁰ If it considers the plans “acceptable,” Transport Canada will “accept” the plans and the freight forwarder will be added to a list of Regulated Agents.¹⁸¹¹ If the plans are “unacceptable,” Transport Canada will request amendments. If agreement cannot be reached on the contents of the plans, Transport Canada will notify the freight forwarder that it will not be added to the list of Regulated Agents.¹⁸¹²

Regulated Agents will be required to maintain secure premises and secure methods of transportation,¹⁸¹³ and will require security clearance checks for employees.¹⁸¹⁴ Regulated Agents must also ensure that all sub-contractors engaged to handle air cargo on their behalf meet the required security standards.¹⁸¹⁵ Given the grave risks presented by air cargo, it is imperative that

¹⁸⁰⁵ Final Submissions of the Attorney General of Canada, Vol. II, para. 358.

¹⁸⁰⁶ Exhibit P-419.

¹⁸⁰⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5190.

¹⁸⁰⁸ Exhibit P-422, pp. 6-8.

¹⁸⁰⁹ Exhibit P-423.

¹⁸¹⁰ The Air Cargo Security Plans must contain the elements outlined in the Transport Canada “Air Cargo Security Plan Required Elements,” as amended from time to time. See Exhibit P-423, clause 5, p. 8.

¹⁸¹¹ Exhibit P-423, clause 9(a), p. 8.

¹⁸¹² Exhibit P-423, clause 9(b), p. 8.

¹⁸¹³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5189.

¹⁸¹⁴ Exhibit P-101 CAF0827, p. 3.

¹⁸¹⁵ Exhibit P-419.

security clearance checks cover all employees with *potential* access to air cargo, whether or not their work involves direct contact. In addition, access to cargo must be appropriately restricted at all times.

Compliance will be monitored by Transport Canada Security Inspectors, either with or without notice to Regulated Agents.¹⁸¹⁶ Regulated Agents are required to conduct at least one self-audit annually to determine the effectiveness of their Air Cargo Security Plans and their implementation. If the self-audit identifies shortcomings, the Regulated Agent must amend its Air Cargo Security Plans, in consultation with Transport Canada, and resubmit them.¹⁸¹⁷ If Transport Canada Security Inspectors find non-compliance with the Air Cargo Security Plans, "...every effort will be made by the parties to identify a means to correct the non-compliance, whether through an amendment or an interim procedure that ensures an equivalent level of security."¹⁸¹⁸ If an agreement to correct non-compliance cannot be reached, the freight forwarder will be removed from the list of Regulated Agents.¹⁸¹⁹

There is confusion over the status of MOUs. They contain an express provision that they are not binding: "...This MOU is a declaration of intentions by the parties and will not create any binding legal obligations."¹⁸²⁰ However, in its instructions for completing the MOU, Transport Canada states that freight forwarders wishing to participate in the program "...must agree to comply with the terms of this Memorandum of Understanding."¹⁸²¹

The non-binding character of the MOUs and the apparently cautionary use of the term "accept" instead of "approve" (when Transport Canada is responding to an Air Cargo Security Plan that is presented to it) are troublesome, especially in light of the evidence before the Commission and the lessons learned from the loss of Air India Flight 182. The current system is reminiscent of the system that was in place for air carrier security plans in 1985.¹⁸²² An insufficient inspectorate existed in 1985, one that was "...thinly stretched for the tasks and the breadth of the industry they were responsible for monitoring."¹⁸²³ In 1985, the system was really one of voluntary compliance, with no true enforcement mechanism.

The language used in the MOUs, which speak of security plans being "accepted," is imprecise. It is not clear what this term means. As demonstrated by the Air India bombings, it is important that security plans obtain formal *approval* by Transport Canada, and that both parties to the agreement are held to their respective responsibilities. At the very least, this demands a binding agreement. The Commission believes that this relationship is best governed by regulation.

¹⁸¹⁶ Exhibit P-423, clauses 13, 14, p. 9.

¹⁸¹⁷ Exhibit P-423, clause 15, p. 9.

¹⁸¹⁸ Exhibit P-423, clause 16, p. 9.

¹⁸¹⁹ Exhibit P-423, clause 19, p. 10.

¹⁸²⁰ Exhibit P-423, p. 11.

¹⁸²¹ Exhibit P-423, p. 4.

¹⁸²² Exhibit P-157, p. 54 of 135.

¹⁸²³ Exhibit P-157, p. 22 of 135.

Transport Canada has indicated, however, that MOUs may continue to govern the security plan requirements when the program is fully implemented. Without a legislated ability to enforce the MOUs, meaningful oversight by Transport Canada is difficult, as it was with air carrier security plans before Flight 182 was bombed.

Under the MOU, it appears that removing a Regulated Agent from the list for non-compliance would only occur as a last resort, where consultations between the two parties fail. Sweet testified that when measures are voluntary, compliance cannot be guaranteed.¹⁸²⁴ A regulatory regime would be preferable.

The Commission is also concerned about quality assurance in the supply chain security system. Conrad testified that there were more than 100 general aviation security inspectors, whose responsibilities included the inspection of air cargo security procedures. Nine additional inspectors were dedicated exclusively to air cargo security.¹⁸²⁵ The Commission did not hear evidence about the adequacy of inspectorate resources at Transport Canada, or about the training and education that will be provided for the full implementation of the additional duties created by a new air cargo security regime. Transport Canada suggested that government-certified bodies might assist in cargo security inspections for industry participants.

In 2005, the report of the US GAO stated that the TSA conducts compliance inspections of air carriers and indirect air carriers. The report noted, however, that the TSA had not "... determined what constitutes an acceptable level of performance or compared air carriers and indirect air carriers' performance against this standard, analyzed the results of inspections to systematically target future inspections on those entities that pose a higher security risk to the domestic air cargo system, or assessed the effectiveness of its enforcement actions taken against air carriers and indirect air carriers to ensure that they are complying with air cargo security requirements."¹⁸²⁶ The report also expressed concern that the TSA had not defined what constitutes a breach of air cargo security, despite having defined breaches in other areas, including passenger and airport access controls.

The ACS Initiative has not been finalized. The concerns expressed about similar systems in the United States may provide useful insights.

3.8.1.4.3 Improving Air Cargo Screening: Use of Technology

The second branch of the ACS Initiative is focused on improving air cargo screening,¹⁸²⁷ in the broadest sense of this term, particularly for high risk

¹⁸²⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4948.

¹⁸²⁵ Exhibit P-101 CAF0872, p. 2.

¹⁸²⁶ Exhibit P-417, p. 6.

¹⁸²⁷ Exhibit P-189, p. 3.

or targeted cargo.¹⁸²⁸ Transport Canada is currently evaluating and testing technology for screening and searching air cargo.¹⁸²⁹

Under the new ACS Initiative, the aim is to screen or search cargo that is loaded on passenger aircraft to a level comparable to that of HBS.¹⁸³⁰ Since January 1, 2006, 100 per cent of hold baggage placed on passenger aircraft and departing from Canada's 89 designated airports has been screened using explosives detection equipment, as required by Annex 17 of the *Chicago Convention*.¹⁸³¹ The screening process involves up to five levels of inspection performed by "state-of-the-art" equipment and screening officers. Among the types of equipment available are computed tomography (CT) X-ray machines.¹⁸³²

Consistent with its general principles for civil aviation security, Transport Canada advocates a performance-based approach to air cargo screening. The specific methodology may therefore vary as long as the end result is screening that is comparable to HBS.¹⁸³³

Cartwright testified that Transport Canada has been collaborating with the US to determine the suitability of various technologies for specific categories of cargo.¹⁸³⁴ Transport Canada has cooperated in simulated tests, known as "technology readiness evaluations," which involve challenging each technology with approximately 5,000 different materials in various orientations to assess the technology's ability to detect concealed devices. Cartwright stated that this testing has required "...an incredible level of work and effort, so that at the end of the day, we know what would work."¹⁸³⁵

Cartwright said that clusters of products within cargo can facilitate screening once appropriate technology is selected but that, overall, air cargo screening is much more complex than HBS.¹⁸³⁶

Transport Canada indicated that it is engaged in a six-stage process for developing its air cargo screening program:

1. Evaluating technology using simulated tests;¹⁸³⁷
2. Assessing operational environments for testing screening technology;¹⁸³⁸
3. Defining screening models and options for screening;
4. Establishing pilot projects and test beds to assess real-world application of screening technology;

¹⁸²⁸ Final Submissions of the Attorney General of Canada, Vol. II, para. 356.

¹⁸²⁹ Exhibit P-422, p. 15.

¹⁸³⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5204-5205.

¹⁸³¹ Exhibit P-169, p. 61.

¹⁸³² Exhibit P-157, p. 108 of 135.

¹⁸³³ Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5204-5205.

¹⁸³⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5151.

¹⁸³⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5206.

¹⁸³⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5233.

¹⁸³⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5206.

¹⁸³⁸ Exhibit P-422, p. 15.

5. Re-evaluating and revising screening models based on pilot project results; and
6. Implementing a defined air cargo screening program.¹⁸³⁹

Transport Canada appears to have reached the fourth stage of this process for “unconsolidated” cargo, while remaining at the first stage for “consolidated” cargo. It has now completed assessing the various operating environments in which to evaluate screening and inspection technologies and protocols for high-risk and targeted cargo.¹⁸⁴⁰ Screening models for unconsolidated cargo have been completed and a process of validation has begun, but screening technologies for explosives detection in consolidated and palletized cargo are still under development. In its Final Submissions, the Attorney General of Canada advised that, despite legislation in the United States requiring 100 per cent screening of air cargo by 2010,¹⁸⁴¹ it is possible that explosives detection equipment may not be available for operational deployment by that time.¹⁸⁴²

Operational trials are currently taking place in several cargo environments to assess the use of X-ray, trace and various “specialty” solutions.¹⁸⁴³ These projects were to be completed by March 2009.¹⁸⁴⁴ At that time, Transport Canada was to have produced a “matrix of appropriate screening models” for industry members. The matrix was to include non-intrusive elements, including X-ray, trace and canine detection methods, which can be used for special cargo categories where physical inspection could cause damage.¹⁸⁴⁵

Participation in the screening development projects is open to air carriers, freight forwarders and shippers taking part in the supply chain security programs.¹⁸⁴⁶ As with supply chain security, Transport Canada is introducing aspects of the program in phases, based on its priorities.¹⁸⁴⁷ For now, the air cargo screening development program is focusing on:

- Freight forwarders and air carriers;
- Locations both on and off airport premises; and
- Matching equipment to the operating environment and cargo characteristics.¹⁸⁴⁸

¹⁸³⁹ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5206.

¹⁸⁴⁰ Exhibit P-422, p. 15: A few months earlier, the Attorney General of Canada reported that the selection criteria for identifying suitable industry sites to evaluate air cargo screening equipment had been completed. In order to apply the selection criteria, three rounds of cargo data collection (such as size, weight and commodity factors) were also completed. See Final Submissions of the Attorney General of Canada, Vol. II, para. 362.

¹⁸⁴¹ Exhibit P-422, p. 9.

¹⁸⁴² Final Submissions of the Attorney General of Canada, Vol. II, para. 363.

¹⁸⁴³ Final Submissions of the Attorney General of Canada, Vol. II, para. 369.

¹⁸⁴⁴ Final Submissions of the Attorney General of Canada, Vol. II, para. 369.

¹⁸⁴⁵ Exhibit P-419.

¹⁸⁴⁶ Final Submissions of the Attorney General of Canada, Vol. II, para. 356.

¹⁸⁴⁷ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5217.

¹⁸⁴⁸ Exhibit P-422, p. 15.

Cartwright noted that technologies used elsewhere in aviation security, such as for passenger and baggage screening,¹⁸⁴⁹ can work for some aspects of air cargo screening.¹⁸⁵⁰ Transport Canada was working with CATSA to benefit from its expertise.¹⁸⁵¹ He testified that, as technology improves in other sectors, it is important to “close off” remaining security gaps by re-applying as many of the new technologies as is reasonable and feasible to “problem areas” such as air cargo.¹⁸⁵²

Transport Canada is also reviewing possible new applications of older technologies. One currently being considered for air cargo screening is thermal neutron activation (TNA), which has already been deployed as a secondary screening tool in at least one country in the Far East.¹⁸⁵³ TNA technology had been developed before the loss of Pan Am Flight 103 to detect bulk explosives in suitcases. However, it was abandoned after the loss because the technology was unable to detect the minimum threshold level of explosives specified at the time.¹⁸⁵⁴ The technology has since been refined and is being evaluated for use in the secondary screening of air cargo.¹⁸⁵⁵

It is important to coordinate efforts with international partners. Coordination permits the sharing of information about technological advances and accords with one of the key objectives of the overall ACS Initiative, international harmonization.¹⁸⁵⁶ On cargo screening technology issues, Canada is cooperating with the European Civil Aviation Technical Task Force, the aviation experts working group at the Asia-Pacific Economic Cooperation (APEC), and with the TSA and DHS in the United States.

One goal of the ACS Initiative is to establish the most practical method of screening air cargo that is also feasible for business. Cartwright maintained that practices are sustainable if they are viewed as “good business” practices.¹⁸⁵⁷ He stressed that air cargo is a time-critical business.

Cartwright and Conrad acknowledged that enhanced air cargo screening will require paying special attention to training. As with all types of screening, there was a need to guard against screeners becoming complacent or inattentive.¹⁸⁵⁸ Technologies that provide motivation in pre-board and hold bag screening appear to be equally useful for air cargo screening. These include the Threat Image Protection System (TIPS), a software training program that projects fictional images of threat objects within the X-ray image of real baggage, and

¹⁸⁴⁹ Final Submissions of the Attorney General of Canada, Vol. II, para. 364.

¹⁸⁵⁰ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5131.

¹⁸⁵¹ Final Submissions of the Attorney General of Canada, Vol. II, para. 364.

¹⁸⁵² Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5131.

¹⁸⁵³ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5181-5182.

¹⁸⁵⁴ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5128.

¹⁸⁵⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5181-5182.

¹⁸⁵⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5182.

¹⁸⁵⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5203.

¹⁸⁵⁸ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5197.

the X-Ray Tutor (XRT), an interactive computer-based training tool for screening officers.¹⁸⁵⁹

The challenge in applying these motivation-enhancing technologies in air cargo screening is to individualize them to cargo type and to take into account geographic variability of cargo. For example, if cargo containing machinery parts is not encountered at a particular location, presenting a computer image of such parts as part of training will be of little value. The training tools need to be specific to the type of cargo. Conrad advised that this issue is under discussion with other countries.¹⁸⁶⁰

Transport Canada is currently assessing the role that government agencies may play in service delivery, including the potential for CATSA and the CBSA to screen air cargo.¹⁸⁶¹ CATSA is the authority responsible for screening passengers and baggage,¹⁸⁶² but under the current legislation, CATSA's mandate does not include cargo screening.¹⁸⁶³ The CATSA Advisory Panel observed that CATSA would be an appropriate agency to oversee the operational aspects of a new air cargo security regime, including validating the screening practices of shippers¹⁸⁶⁴ and conducting screening-related operations.¹⁸⁶⁵

Cartwright advised that using CATSA equipment is one option being reviewed in the pilot projects. He said that one complicating factor is the Air Travellers Security Charge (ATSC), a fee paid by air travellers to fund security measures, including those provided by CATSA.¹⁸⁶⁶ If CATSA were to become involved in air cargo screening, the ATSC might have the unintended effect of funding the use of CATSA's equipment for air cargo. This issue would need to be resolved. However, this is not a major issue, and it could easily be addressed through greater transparency and accountability relating to the ATSC. Cartwright testified that where CATSA screening equipment is available, such as during idle periods, the possibility of diverting it for screening air cargo cannot be ruled out. For example, CATSA's equipment could be used to screen cargo at airports during the night, when passenger traffic is typically low.¹⁸⁶⁷

Duguay said that CATSA had both the equipment and the expertise to screen air cargo and could do so, at least at the smaller Class 2 airports.¹⁸⁶⁸ He stated that air carriers also possessed the requisite expertise and personnel, since they were currently responsible for air cargo screening. However, he acknowledged that CATSA had the equipment and was already the screening authority for

¹⁸⁵⁹ Exhibit P-169, p. 202 of 202 (Appendix E); Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5198.

¹⁸⁶⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5198.

¹⁸⁶¹ Final Submissions of the Attorney General of Canada, Vol. II, para. 356; see also Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5188-5189.

¹⁸⁶² Exhibit P-169, p. 62 of 202.

¹⁸⁶³ Exhibit P-169, p. 68 of 202.

¹⁸⁶⁴ Exhibit P-169, p. 55 of 202.

¹⁸⁶⁵ Exhibit P-169, p. 69 of 202.

¹⁸⁶⁶ Exhibit P-169, p. 168 of 202.

¹⁸⁶⁷ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5204.

¹⁸⁶⁸ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5261.

both passengers and baggage.¹⁸⁶⁹ As previously noted, Air Canada does not itself have access to equipment for screening air cargo.¹⁸⁷⁰

At most Class 2 airports where Air Canada has cargo facilities or cargo counters, its facilities are located near CATSA HBS operations. Since cargo accepted at these smaller airports tends to be small parcels, the cargo could very well be screened by CATSA using the equipment available.¹⁸⁷¹ However, the effect on throughput at Class 2 airports would need to be evaluated.¹⁸⁷² Duguay stated that using CATSA equipment to screen cargo was possible even at some Class 1 airports, although this would need to be assessed on an individual basis.¹⁸⁷³

Almost a quarter century after the Seaborn Report was released, the recommendation to X-ray small parcels still has not been implemented.¹⁸⁷⁴

Duguay also envisioned a role for CATSA in screening larger cargo at a central location at an airport. With the advent of a supply chain approach to air cargo security, he saw a potential benefit to having a location at an airport where air carriers could bring their shipments to be screened using advanced technology. CATSA would manage and supervise the process. Sophisticated screening equipment would be required and, given the large size of much cargo, could be costly. According to Duguay, it was sensible to centralize such equipment to maximize its use. This was the operational model currently followed in Europe.¹⁸⁷⁵

Conrad stated that while a centralized screening area operated by CATSA or another government entity might be feasible at large airports, it was more problematic for medium-sized and smaller airports. He noted that employing dedicated air cargo screeners required “volumes of scale” that are not present in smaller locations, and that this was not cost-effective. This would require considerable resources and would be extremely complex and difficult to manage from an oversight perspective. Instead, placing responsibility for screening cargo at these locations with a third party, such as an air carrier or freight forwarder, would take advantage of the benefits derived from “multiple duty” workers. He stated that seeking such efficiencies was important “...because in Canada, especially with our sparse population, some of the challenge for us is to make sure that the small and medium size enterprises can still compete within the marketplace and that they’re still able to provide services in a secure and efficient fashion.”¹⁸⁷⁶ Different models may, therefore, be appropriate for different environments.

¹⁸⁶⁹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5259.

¹⁸⁷⁰ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5291.

¹⁸⁷¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5259.

¹⁸⁷² Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5262.

¹⁸⁷³ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5259.

¹⁸⁷⁴ Exhibit P-101 CAF0039, p. 6 of 10.

¹⁸⁷⁵ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5261-5262.

¹⁸⁷⁶ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5218.

Even following the loss of Air India Flight 182, the screening of passengers and baggage remained in the hands of air carriers. As previously noted, the CATSA Advisory Panel identified this as a serious security weakness, since security would not be the carriers' principal concern.¹⁸⁷⁷ When, after the events of September 11th, CATSA was created, responsibility for screening passengers and baggage was removed from the carriers.¹⁸⁷⁸

CATSA might play a prominent role in air cargo security. Air cargo screening would be a natural extension of its existing passenger, non-passenger and baggage screening duties. CATSA has the expertise, equipment and dedicated personnel, and is already familiar with the training models that Transport Canada would modify for air cargo screening. CATSA could provide full or "residual" screening services at airports, particularly for small cargo, and might also be involved in oversight and inspection of supply chain participants.¹⁸⁷⁹ CATSA could also provide centralized screening services for bulkier cargo at larger airports.

At smaller airports, centralized screening areas for larger cargo may be less practical. Still, facilities may be needed for screening or searching cargo. It might be more appropriate for freight forwarders or even shippers to perform screening or searching at their premises prior to consolidation or packaging. However, under Transport Canada's proposed program, air carriers would retain ultimate responsibility for the security of air cargo. The carriers must have the means to satisfy themselves that cargo is secure.¹⁸⁸⁰

Because the screening of passengers, non-passengers, baggage and cargo involves overlapping skills, it might be more efficient for CATSA, rather than air carriers, to conduct cargo screening. Oversight by Transport Canada or a third party would be required, regardless of the entity – CATSA or an air carrier – delivering the screening service.

The only issue that appears to differentiate the two delivery modes – CATSA or the air carriers – for screening at smaller airports is the assumption of costs. It may be expensive, either for an air carrier or for CATSA, to maintain facilities for screening larger cargo at small airports. No evidence was presented to the Commission about how to apportion the costs.

3.8.1.4.4 Funding

The ACS Initiative proposes to establish a nationwide regulatory framework for a long-neglected sector of aviation security. Conrad testified that oversight and

¹⁸⁷⁷ Exhibit P-157, p. 67 of 135.

¹⁸⁷⁸ Exhibit P-157, p. 67 of 135.

¹⁸⁷⁹ Exhibit P-169, p. 55 of 202.

¹⁸⁸⁰ It should be remembered that the regulated agent program, if implemented as envisaged by ICAO, should enable airline checks of cargo coming from such agents to be limited to a 'documentary' check, including checks of seals. Cargo delivered by non-regulated agents – e.g. a passenger shipping baggage ahead of the passenger's flight (in which case it becomes cargo), or an unknown intending shipper arriving at a cargo shed – would have to be screened by the airline or an agency, perhaps CATSA, acting on the airline's behalf.

monitoring compliance with the new regime, still a work in progress,¹⁸⁸¹ would involve significant ongoing costs.¹⁸⁸² Robust air cargo security was dependent upon sufficient and sustained funding.

Transport Canada identified financial sustainability as one of its key objectives in developing the ACS Initiative.¹⁸⁸³ Conrad recognized that government and industry have limited resources. Several models were being considered, including government funding, industry funding and user-pay formulas.¹⁸⁸⁴ Conrad stated that, based on the Government's previous experience in funding aviation security measures, a user-pay model was likely. Since the "user" in the air cargo industry was primarily the shipper, much of the cost in this model would be borne by the shipper.¹⁸⁸⁵

If a user-pay model is adopted, industry resistance can be expected. This has already been seen with the ATSC, a fee levied on air travellers to fund enhanced aviation security initiatives, including the creation of CATSA. The ATSC came into effect in April 2002 and faced sharp criticism by industry stakeholders.¹⁸⁸⁶ The Canadian Airports Council (CAC), the Air Transport Association of Canada (ATAC), airport authorities and air carriers all strongly opposed the ATSC. They argued that the purpose of the ATSC was the protection of national security and that, for this reason, costs should be borne by government, not by the civil aviation industry or passengers. Concerns have also been raised by industry stakeholders about the lack of transparency and accountability surrounding the use of funds generated by the ATSC.¹⁸⁸⁷

The question of who should pay is not new. In 1993, Wallis anticipated that airlines might not immediately support enhanced security requirements for cargo, noting that "...[t]he carriage of freight in the hold of passenger aircraft provides a very valuable contribution to an airline's income."¹⁸⁸⁸ Purolator, Canada's largest courier company,¹⁸⁸⁹ addressed costs during to the *CATSA Act* Review consultation process in June 2006. In a letter to the Review Secretariat, the Director of Security and Regulatory Affairs for Purolator called for government to bear the costs:

...[I]t is Purolator's position that while industry participants (e.g. air carriers, freight forwarders, shipper and airports) must share a collective responsibility in effecting compliance with mandated national air cargo security measures, the costs

¹⁸⁸¹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5200.

¹⁸⁸² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5200.

¹⁸⁸³ Exhibit P-189, p. 4.

¹⁸⁸⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5186.

¹⁸⁸⁵ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5201.

¹⁸⁸⁶ Exhibit P-169, p. 168 of 202.

¹⁸⁸⁷ Exhibit P-169, p. 169 of 202.

¹⁸⁸⁸ Wallis, *Combating Air Terrorism*, p. 79.

¹⁸⁸⁹ Exhibit P-191, p. 1.

associated with achieving such compliance, as in all matters of national security, are rightly borne by the Government of Canada.

The ATSC for passengers can be distinguished from a user-pay model for air cargo. Air cargo in Canada is carried primarily on passenger aircraft, but does not necessarily have a direct connection to the passengers on the flight, unlike hold baggage, for example. Air cargo security measures may benefit passengers, but the presence of air cargo on board aircraft is not, for the most part, for their specific advantage. In fact, air cargo carried on passenger flights endangers passengers and crew if adequate security controls are not applied.

Air cargo is carried on passenger aircraft to facilitate trade.¹⁸⁹⁰ Air carriers showed little interest in air cargo until its revenue potential became apparent. Air carriers then began to make strenuous efforts to sell their aircraft hold capacity.¹⁸⁹¹ Security for air cargo also directly benefits the industry by protecting valuable goods against sabotage.

How to obtain sustainable funding for air cargo security is critical. Air cargo security, like pre-board screening (PBS), HBS and NPS, is a key component of aviation security. It is imperative that any air cargo security program remains intact even in difficult economic or political circumstances.

Using a risk-based analysis, air cargo is one of the major domains of risk in civil aviation.¹⁸⁹² Consequently, despite limited resources, sufficient funds must be allocated to air cargo screening – ideally to a level that reflects the ALARA principle (“as low as reasonably achievable”).¹⁸⁹³

Sustained funding for air cargo security also has implications for Transport Canada’s stated objectives of interoperability¹⁸⁹⁴ and international harmonization.¹⁸⁹⁵ Air cargo represents a significant portion of Canada’s trade, and both domestic and international partners will come to rely on a consistent air cargo security regime. Countries with air cargo security programs will no doubt expect Canada to maintain a comparable system, and Canada will expect the same of others.¹⁸⁹⁶

Canada is a member of the G8 and is among the wealthiest nations in the world. Transport Canada claims that Canada prides itself as a leader in international civil aviation security.¹⁸⁹⁷ As Wallis noted, wealthy industrialized nations such as Canada should be able to go well beyond the lowest-common-denominator

¹⁸⁹⁰ Exhibit P-169, p. 52 of 202.

¹⁸⁹¹ Wallis, *Combating Air Terrorism*, p. 79.

¹⁸⁹² Testimony of William Leiss, vol. 91, December 7, 2007, p. 11960.

¹⁸⁹³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11961.

¹⁸⁹⁴ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5186.

¹⁸⁹⁵ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5182.

¹⁸⁹⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, p. 5183.

¹⁸⁹⁷ Exhibit P-419.

standards of Annex 17 of the *Chicago Convention*. If Canada is seen to have difficulty sustaining funding for air cargo screening, it will be hard pressed to ask less wealthy nations to apply similar measures.

IATA recently reported that the international airline industry faces a grim outlook, with soaring fuel costs and economic turmoil reducing passenger numbers.¹⁸⁹⁸ Measures must be taken to prevent the dismantling of funding for air cargo security in times of economic downturn.

3.8.1.5 A Call for Action from the Government of Canada

The vulnerability of air cargo to sabotage and the potential consequences to aviation security were brought to the Government's attention as early as 1980. It was not until 2004 that the Government formally acknowledged the need to address deficiencies in air cargo security. At that time, Transport Canada began to develop a program to rectify some deficiencies. In 2006, \$26 million was allocated to the development and pilot-testing of an enhanced air cargo security regime, scheduled to be completed in 2008-09. By 2008, pilot testing of the program's initiatives had just begun and cargo carried on passenger aircraft remained largely unsearched, and thus vulnerable to sabotage. Work to improve air cargo security must be accelerated.

Conrad testified that improving air cargo security was a complicated task, but said that progress was being made:

[T]here [have] been lots of comments made that we should certainly move quicker and...we should put more things in place faster and one of the things, I think is important to note...if there were very simple solutions that we felt that would get us to significant improvement today, I think we would have done them. But I think the reality is...that there's a lot of good things that have been taking place and I think we are on a really strong path that in a fairly short timeframe we're going to make significant strides in improving air cargo security within Canada.¹⁸⁹⁹

Many years have passed since the bombing of Air India Flight 182 and since the international civil aviation community established the regulated agents model for air cargo security. Still, air cargo in Canada has been permitted on passenger flights with little in the way of security controls. It is no answer after all this time to say that delay is warranted because of the complexities of air cargo screening.

¹⁸⁹⁸ Exhibit P-424, p. 1 of 2.

¹⁸⁹⁹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5199.

Canada was quick to recognize gaps in passenger and baggage screening. When CATSA was created in 2002, its mandate was to provide screening solely for passengers and their baggage. Not long afterwards, in November 2002, the Minister of Transport assigned two further functions to CATSA. One was the screening of non-passengers who enter restricted areas of airports, along with any items carried.¹⁹⁰⁰ Non-passengers who have access to restricted areas can potentially plant bombs on aircraft.

Conrad conceded that air cargo, although recognized as vulnerable to sabotage, was ignored in the past due to limited resources:

Not to say that we don't acknowledge an area of risk, but when we look at prioritizing and putting resources into those areas, when it came to moving on hold baggage, we certainly – within the resource constraints of what we had at the time, we certainly recognize that we had to get that done. Not that we wanted to avoid doing cargo, but within the resource envelope that we had, we certainly had to make some decisions in terms of where we could put the resources first.¹⁹⁰¹

Leiss said this reasoning was flawed. One area of risk must not be ignored while managing another, particularly where the risk being ignored is a high priority risk.¹⁹⁰² This is irresponsible risk management. While resources will always be limited,¹⁹⁰³ all risks must be managed to an acceptable level within the available budget.¹⁹⁰⁴ Conrad's statement suggests that a conscious decision was made not to allocate resources to air cargo security, despite knowledge of the risk. Perhaps Transport Canada decided to forego air cargo screening in favour of passenger and baggage screening because it considered the risk posed by air cargo to be acceptable. The many industry stakeholders and experts who appeared before the Commission would disagree. The Senate Committee would likely consider the conclusion that the risk posed by air cargo was acceptable to be an example of trade and efficiency concerns inappropriately trumping necessary security.¹⁹⁰⁵

Cartwright testified that many countries were struggling with air cargo security issues:

The point I was trying to make is they, along with a number of other areas of the world, are struggling with the same things we are, and that is how to put together a program that is cohesive, integrated and has the capabilities and produces the

¹⁹⁰⁰ Exhibit P-169, p. 61 of 202.

¹⁹⁰¹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5212.

¹⁹⁰² Exhibit P-361, Tab 1, p. 3 of 12.

¹⁹⁰³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11990.

¹⁹⁰⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 11992.

¹⁹⁰⁵ Exhibit P-172, p. 42 of 155.

performance that we all want. So could we have done more? I'm sure we could have done. Can we do more? I'm sure we will. But the issue is I don't know that we are as far behind as is sometimes portrayed. Again, can we do more? Sure we can. But...other countries are struggling with the same kinds of issues and that's hence the collaboration...in doing the data gathering, so that we all work from a common data set, so we make the decisions in the same way. We may not make the same decisions but we will be basing it on a common data set of what doesn't work for which types of cargo.¹⁹⁰⁶

The fact that other countries have also failed to address an area of aviation security that Canada has identified as severely deficient should not determine the pace of Canada's progress on security policies or protocols, nor should it justify inaction. Many countries have long-established, highly-lauded air cargo security programs. The UK, for example, produced regulations for a regulated agent program by 1993, shortly after the concept was incorporated into Annex 17.¹⁹⁰⁷ International harmonization to the lowest common denominator – in this case, inaction on air cargo security – is not acceptable for Canada. If Canada indeed has "...one of the best aviation safety and security programs in the world,"¹⁹⁰⁸ it must move far beyond the lowest common denominator in air cargo security.

Similar, though less protracted, delays weakened aviation security in 1985. As is the case today, Transport Canada was well aware by 1985 of gaps within its aviation security system and "...had work under way to correct them."¹⁹⁰⁹ This work included legislative initiatives. At the time of the Air India bombing, draft regulations prescribing security measures for a new category of "special risk" flights had been circulating in government for three years, but had not been implemented.¹⁹¹⁰ Had the draft regulations been in effect in June 1985, they would have applied to Air India, which was clearly facing an elevated threat.¹⁹¹¹ In addition, at the time of the Air India bombing, a bill to amend the *Aeronautics Act* was before Parliament. The bill would have given the Minister of Transport the power to prescribe new procedures for preventing unlawful interference with civil aviation.

By June 1985, Transport Canada had been working closely with the National Research Council "for some time" to develop explosives vapour detection systems for screening checked baggage, but these were not yet considered ready for use at Canadian airports. A similar situation exists today, with cargo screening technology, including explosives detection systems, under evaluation while

¹⁹⁰⁶ Testimony of Nick Cartwright, vol. 42, June 13, 2007, pp. 5219- 5220.

¹⁹⁰⁷ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5003.

¹⁹⁰⁸ Exhibit P-419.

¹⁹⁰⁹ Exhibit P-157, p. 55 of 135.

¹⁹¹⁰ Exhibit P-157, p. 57 of 135.

¹⁹¹¹ Exhibit P-157, p. 57 of 135.

cargo remains largely unsearched. The CATSA Advisory Panel reported that "...[i]mmediately following the Air India tragedy, the department expedited the acquisition and installation of 26 [explosives vapour detection] units at major Canadian airports." Equipment that the Department had concluded was not ready for use on June 22, 1985, was suddenly approved for deployment across the country in the wake of the Air India bombing. This serves as a cautionary tale for air cargo. Air cargo in Canada is primed and ready for sabotage, while at the same time the technology that could help to prevent that sabotage is being withheld from service until it is further refined.

Transport Canada posted the following about the ACS Initiative on its website:

Working with the aviation and cargo industries, Transport Canada's goal is to develop and enhance a comprehensive Air Cargo Security program that meets the highest standards in the world, assures the safety and security of the traveling public, and facilitates the efficient flow of goods in and out of Canada.¹⁹¹²

As Wallis stated upon hearing accolades bestowed upon attendees at a ministerial conference for aviation security, there is a need to ensure that these are not just more "words, words, words."¹⁹¹³

The CATSA Advisory Panel noted that the "...slow progress in completing security projects continues today to be a risk factor for Canada as it leaves significant known gaps unclosed. This points to a need for Transport Canada to adopt interim measures to fill known gaps while more comprehensive solutions are being developed."¹⁹¹⁴

Canada could implement several measures relatively quickly, such as using CATSA equipment to X-ray small cargo packages and conducting physical searches of larger cargo. Yet the Government has failed to take decisive action. While comprehensive improvements to air cargo security may require time, interim procedures such as those mentioned in this paragraph could provide an important, if incomplete, layer of security. As security measures and technology develop, the gaps in security will diminish. In the meantime, gaps must be addressed with the measures that are currently available.

Interim measures for searching air cargo have been put in place in the United States while more advanced technology is being developed.¹⁹¹⁵ As well, TSA officials advised that, in the absence of formal vulnerability and criticality assessments, they would continue to use available threat intelligence, expert judgment and information about past terrorist incidents to select and prioritize air cargo security efforts, including how best to distribute the TSA security

¹⁹¹² Exhibit P-419.

¹⁹¹³ Testimony of Rodney Wallis, vol. 39, June 4, 2007, p. 4722.

¹⁹¹⁴ Exhibit P-157, p. 67 of 135.

¹⁹¹⁵ Exhibit P-417, p. 53.

inspectorate.¹⁹¹⁶ The TSA also considered random cargo inspections to be interim measures.¹⁹¹⁷

Wallis described action on air cargo security as long overdue:

So again, discussions on these issues have been around a long time. One of the problems is that discussions go on and on, and on and on and people don't act. People have to act. And I think that we are at the time when in the cargo scene, for example, action is called for and governments should be looking at that particular operation.¹⁹¹⁸

Industry stakeholders, aviation security experts and the Government of Canada agree that air cargo security is among the weakest links in the aviation security chain. The Government must discharge its responsibility to address this weakness.

3.8.1.6 Conclusion

Terrorists probe for weaknesses in aviation security. For decades, air cargo has been known to be such a weakness. Today most industry experts and stakeholders consider it the most significant vulnerability in civil aviation security. The existing security regime places civil aviation at grave risk. There is little screening of those who present cargo for transport and very little cargo is searched before it is carried on aircraft. Almost 80 per cent of air cargo travels on passenger aircraft.

Despite knowledge of this serious vulnerability, the Government of Canada has failed to introduce appropriate security measures.

The ACS Initiative is a promising and welcome start. A long overdue system of regulated agents to secure air cargo along the supply chain, coupled with what appears to be a comprehensive plan to screen and search all air cargo, will go a long way towards preventing sabotage. Still, the lessons of Air India Flight 182 need to be kept in mind, and potential weaknesses in the new air cargo screening regime must be anticipated to the extent possible and addressed quickly. Models for delivering screening services, including the potential involvement of CATSA, require thoughtful consideration. Training protocols and access control must be meaningful and thorough.

¹⁹¹⁶ Exhibit P-417, p. 28.

¹⁹¹⁷ Exhibit P-417, p. 29.

¹⁹¹⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5010.

Sustainable funding for air cargo security is also imperative. Air cargo security represents a vital component of the overall aviation security regime. It must not be allowed to be weakened by lack of funding or political circumstances.

Almost three decades have passed since air cargo security was recognized as a concern. Interim measures are crucial while permanent solutions are being determined. As recommended in 1985 by the Seaborn Report, small packages should be X-rayed immediately, using existing equipment. Physical searches of consolidated cargo should also be conducted on a random and targeted basis. Transport Canada should accelerate its program for selecting and deploying technology for searching air cargo.

3.8.2 Airport Security

Like screening programs, measures to protect the airport environment are essential. Airports represent the hub of civil aviation, where industry, the government and the public interact.¹⁹¹⁹ Almost all aviation security measures, including passenger and baggage screening, are conducted at the airport.¹⁹²⁰ The airport functions as a physical barrier protecting the aircraft. Under a multi-layered approach to security, the airport must complement and preserve the integrity of all other security measures. Otherwise, the aircraft, its passengers and crew are vulnerable.

However, the Commission learned that there have long been significant deficiencies in Canadian airport security. In particular, access to airside and restricted areas of airports is poorly controlled. Financial resources have been directed primarily at strengthening passenger and baggage security.¹⁹²¹ As a result, unlike the comprehensive, multi-tiered screening process that

¹⁹¹⁹ The primary industry and government organizations are the airport operator, Transport Canada, air carriers, CATSA and the police of local jurisdiction. At eight Class 1 designated airports, there are heightened security requirements and therefore a greater presence of RCMP officers dealing with non-aviation security matters. CSIS also maintains offices on site at some international airports. In addition, there are many airport tenants, often consisting of commercial establishments whose purposes are unrelated to aviation security. See Exhibit P-169, pp. 49-50 of 202.

¹⁹²⁰ Under the proposed Air Cargo Security (ACS) Initiative, government-regulated shippers and freight forwarders would apply security measures to air cargo prior to its arrival at the airport. Such a system would notionally extend the perimeter of the airport by securing air cargo through its supply chain, rather than at the airport. See, generally, Exhibit P-422; see also Testimony of Stephen Conrad, Vol. 42, June 13, 2007, p. 5185.

¹⁹²¹ In 2005, the Auditor General of Canada reported that Budget 2001 "had emphasized passengers as the key risk and the Budget had directed funding only to passenger transportation." See Exhibit P-411, p. 9. Budget 2009 also appeared to be heavily weighted towards passenger and baggage security, pledging funds to assist CATSA, which it described simply as "providing consistent and rigorous screening of passengers and baggage," and announcing the implementation of "a new passenger assessment system." However, funding was also announced to support a new program for air cargo security. See Exhibit P-407. In May 2009, a Transport Canada news release provided more details about the breakdown of funding for aviation security from Budget 2009: \$2.9 million is to be set aside for the development of aviation security plans, with the priority for the coming year being airport security plans. Of \$355.8 million earmarked for CATSA, \$9.2 million will fund "non-passenger and vehicle access control and screening at critical restricted areas of airports, using biometric identification technology." By contrast, approximately \$82 million of this funding will go towards upgrading equipment for screening passengers and baggage at Canadian airports.

passengers and their baggage undergo in the airport terminal,¹⁹²² the process applied to non-passengers who obtain access to restricted areas of airports, along with their belongings, lacks rigour and can easily be circumvented.¹⁹²³ Lax perimeter security allows vehicles and their occupants to enter airside portions of the airport with minimal, if any, screening.¹⁹²⁴ There is evidence to suggest that, once on airport property, the movement of such vehicles is not carefully monitored. As a result, despite impressive efforts to safeguard the aircraft against sabotage from passengers and baggage, many opportunities remain to place bombs aboard aircraft. Even publicly-accessible areas of air terminal buildings are susceptible to attack by terrorists, who seek large gatherings of people in confined areas to achieve the greatest impact.¹⁹²⁵

Rodney Wallis, former Director of Security at the International Air Transport Association (IATA) and an international civil aviation security consultant, wrote that the events of September 11, 2001, “questioned, as no other event ever could, the adequacy of airport security in North America.”¹⁹²⁶

In Canada, the Air India bombings of June 23, 1985, revealed important weaknesses in airport security, including problems with access control, airport security plans, perimeter security and general security awareness.¹⁹²⁷ By August 1985, an action plan was developed to address these shortcomings.¹⁹²⁸ The terrorist attacks of September 11th led to the creation of a Crown corporation, the Canadian Air Transport Security Authority (CATSA), which was given the responsibility for screening non-passengers and for developing the biometric Restricted Area Identification Card (RAIC).¹⁹²⁹

Despite these improvements, many airport security deficiencies identified in 1985 continue to be cited as major problems that urgently need to be addressed.¹⁹³⁰

Weaknesses in airport security, together with shortcomings in air cargo,¹⁹³¹ Fixed Base Operation (FBO) and General Aviation (GA) security,¹⁹³² have led to a system in which fortress-like security is applied to the more public, visible side of aviation, while the less visible side remains exposed to possible attack. As mentioned elsewhere in this volume, the Standing Senate Committee on National Security and Defence (Senate Committee) likened the current status of aviation security in Canada to a house in which “...the front door...[is] fairly well

¹⁹²² See Section 3.5 for a description of screening procedures currently in place for passengers and baggage.

¹⁹²³ Exhibit P-169, p. 58 of 202.

¹⁹²⁴ Final Submissions of the Attorney General of Canada, Vol. II, para. 380.

¹⁹²⁵ Exhibit P-169, p. 57 of 202.

¹⁹²⁶ Wallis, *How Safe Are Our Skies?*, p. 65.

¹⁹²⁷ Exhibit P-101 CAF0695, pp. 1, 3 of 3; see also Exhibit P-457, pp. 11, 20 of 27.

¹⁹²⁸ Exhibit P-101 CAF0695, p. 3 of 3.

¹⁹²⁹ Exhibit P-169, pp. 16, 67 and 73 of 202.

¹⁹³⁰ See, for example, Exhibit P-169, p. 58 of 202.

¹⁹³¹ See Section 3.8.1 for a detailed analysis of the deficiencies in the current air cargo security regime.

¹⁹³² See Section 3.8.3 for a detailed analysis of the security deficiencies at FBOs and in the GA sector.

secured, with the side and back doors wide open.”¹⁹³³ The protection provided by the full passenger and baggage security screening is diluted by porous security in other areas of airport operations.

3.8.2.1 Air India Flight 182: Airport Security Deficiencies Revealed

The Commission was surprised to learn about how long Canada has known of many weaknesses in airport security that persist today. The bombing of Flight 182 exposed widespread deficiencies in aviation security, among them deficiencies at airports. This sparked change, both in Canada and on the international stage.

Within days of the bombing, IATA, a trade association for the world’s international scheduled airlines,¹⁹³⁴ convened an extraordinary meeting of its Security Advisory Committee (SAC) to assess the gaps in security procedures that had been revealed.¹⁹³⁵ Ramp security was identified as one gap.¹⁹³⁶ The ramp is the area of the airport where the physical handling of the aircraft takes place.¹⁹³⁷ A working group of security specialists on ramp security was subsequently established to consider measures to better protect the ramp from infiltration by terrorists. The working group presented its findings to the SAC in September 1985.¹⁹³⁸

Following the loss of Flight 182, airport security also became a priority in Canada. On July 4, 1985, Transport Canada’s Deputy Minister requested an audit of airport security at Vancouver, Pearson and Mirabel International Airports¹⁹³⁹ – the airports through which the bomb had journeyed.¹⁹⁴⁰ The audit report was completed on July 24, 1985,¹⁹⁴¹ and revealed serious deficiencies at all three airports. Common among the deficiencies were inadequate protection of the aircraft, inadequate control of access to restricted areas, deficiencies in airport security plans, and insufficient security awareness among employees.¹⁹⁴² Experts continue to highlight these as problems today.

The report cited specific examples of parked aircraft that were often not locked or secured,¹⁹⁴³ airport security plans that were not up to date,¹⁹⁴⁴ restricted areas with

¹⁹³³ Exhibit P-171, p. 13 of 256; see also Exhibit P-172, p. 30 of 155.

¹⁹³⁴ Wallis, *Combating Air Terrorism*, p. 102.

¹⁹³⁵ Wallis, *Combating Air Terrorism*, p. 5.

¹⁹³⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4476-4477.

¹⁹³⁷ Wallis, *Combating Air Terrorism*, p. 59.

¹⁹³⁸ Testimony of Rodney Wallis, vol. 37, May 31, 2007, pp. 4476-4477.

¹⁹³⁹ Exhibit P-457, p. 3 of 27; The resulting audit report, dated July 25, 1985, had been labeled with the note: “Report prepared for Department of Justice Counsel Assessing the Potential for Litigation.”

See Exhibit P-457, p. 1 of 27.

¹⁹⁴⁰ Exhibit P-157, p. 11 of 135.

¹⁹⁴¹ Exhibit P-457, p. 1 of 27.

¹⁹⁴² Exhibit P-101 CAF0695, p. 1 of 3; see also Exhibit P-457, pp. 11, 20 of 27.

¹⁹⁴³ Exhibit P-457, pp. 11-12 of 27.

¹⁹⁴⁴ Exhibit P-457, pp. 12 and 21 of 27.

open and insecure doors,¹⁹⁴⁵ easily breached locks,¹⁹⁴⁶ non-standard perimeter fencing¹⁹⁴⁷ and inadequate control and inspection of employee identification passes.¹⁹⁴⁸ The report noted that unscreened passengers arriving from feeder airports were able to enter “sterile” areas of these major airports.¹⁹⁴⁹ Some of the most egregious security breaches were found at Toronto’s Pearson Airport. They included “several thousand”¹⁹⁵⁰ personnel identification passes which could not be accounted for because they had been stolen, lost or not returned, and restricted area entry doors that could be unlocked by inserting a credit card or because the lock combination was written on the doors themselves.¹⁹⁵¹ The report also noted that access to aircraft by personnel such as caterers and groomers was not closely monitored at Pearson, nor was it normal practice to inspect food delivered to the aircraft or perform a search of the aircraft once all support personnel had deplaned.¹⁹⁵² The ability to control restricted areas at Pearson was considered “highly suspect,”¹⁹⁵³ and unauthorized access to aircraft had occurred.¹⁹⁵⁴ Among the security weaknesses found at Mirabel Airport in Montreal were airport passes that were not always worn in cargo handling areas¹⁹⁵⁵ and air cargo areas that could be “penetrated almost at will.”¹⁹⁵⁶

In most instances, the problem was not a complete absence of security measures. Measures were in place, but did not adequately address the security concern, or their application was insufficiently monitored¹⁹⁵⁷:

...[A]lthough restricted areas are established and physical measures have been implemented to supplement the policing function, many areas still remain vulnerable to determined and even accidental entry.¹⁹⁵⁸

Shortly after completion of the airport security audit, the Canadian Air Transportation Administration addressed a memorandum, dated August 19, 1985, to Transport Canada’s Deputy Minister. The memorandum stated that corrective action was being taken to deal with the deficiencies identified by the review.¹⁹⁵⁹ These actions included facility improvements and repairs, increased monitoring and inspection, increased vigilance and improved security controls

¹⁹⁴⁵ Exhibit P-101 CAF0695, p. 1 of 3.

¹⁹⁴⁶ Exhibit P-457, p. 14 of 27.

¹⁹⁴⁷ Exhibit P-457, p. 14 of 27.

¹⁹⁴⁸ Exhibit P-457, pp. 13 and 24 of 27.

¹⁹⁴⁹ Exhibit P-457, p. 18 of 27.

¹⁹⁵⁰ Exhibit P-457, p. 13 of 27.

¹⁹⁵¹ Exhibit P-457, pp. 13-14 of 27.

¹⁹⁵² Exhibit P-457, p. 20 of 27.

¹⁹⁵³ Exhibit P-457, p. 20 of 27.

¹⁹⁵⁴ Exhibit P-457, p. 20 of 27.

¹⁹⁵⁵ Exhibit P-457, p. 24 of 27.

¹⁹⁵⁶ Exhibit P-457, p. 23 of 27.

¹⁹⁵⁷ Exhibit P-101 CAF0695, p. 2 of 3.

¹⁹⁵⁸ This comment referred to security measures at Pearson International Airport in Toronto: Exhibit P-457, p. 14 of 27.

¹⁹⁵⁹ Exhibit P-101 CAF0695, p. 3 of 3.

for parked aircraft,¹⁹⁶⁰ updated airport security plans,¹⁹⁶¹ and the development of a security awareness program for airport workers and airport users.¹⁹⁶² The memorandum said actions on these matters were "...being undertaken on a high-priority basis."¹⁹⁶³

The Government of Canada also commissioned a more holistic review of airport and airline security in Canada, prompted directly by the loss of Air India Flight 182.¹⁹⁶⁴ Known as the Seaborn Report, its findings were released on September 24, 1985. The report acknowledged the recent audit of airports in Vancouver, Toronto and Montreal that had uncovered "...gaps in the security net, particularly respecting possible unauthorized access to the airfield and the airside portion of the terminal."¹⁹⁶⁵ The report made recommendations for improving airport security, including:

- the need for security and criminal background checks, as a condition of employment, for all airside employees and others with access to sensitive areas of the airport or aircraft;
- requiring airport workers to wear clearly visible and controlled identification at all times;
- requiring airport management to instill in all workers a high level of security awareness throughout the airport and on the airfield, as a priority; and
- the need for public awareness of the security measures in place for its protection at airports and of the contribution the public could make to enhancing security.¹⁹⁶⁶

Almost a quarter century later, many of the deficiencies noted by the airport security audit report and the Seaborn Report, including inadequate access control, remain urgent concerns. Many of the solutions proposed for bringing airport security to an appropriate standard are the same as well.¹⁹⁶⁷ The Commission notes that the 2009 Budget announced \$2.9 million in funding for the development of aviation security plans, with priority being given to the "initiation of airport security plans"¹⁹⁶⁸ as a result of pilot projects conducted at several airports in the past year. The Budget also provided funding to hire additional oversight officers. Virtually all stakeholders and experts recommended

¹⁹⁶⁰ Exhibit P-101 CAF0695, pp. 1-2 of 3.

¹⁹⁶¹ Exhibit P-101 CAF0695, p. 2 of 3.

¹⁹⁶² Exhibit P-101 CAF0695, p. 3 of 3.

¹⁹⁶³ Exhibit P-101 CAF0695, p. 3 of 3.

¹⁹⁶⁴ Exhibit P-101 CAF0039, p. 1 of 10.

¹⁹⁶⁵ Exhibit P-101 CAF0039, p. 8 of 10.

¹⁹⁶⁶ Exhibit P-101 CAF0039, p. 8 of 10.

¹⁹⁶⁷ Exhibit P-169, p. 58 of 202.

¹⁹⁶⁸ "Government of Canada Invests in Aviation Security" (Transport Canada News Release: May 4, 2009), online: Transport Canada < <http://www.tc.gc.ca/mediaroom/releases/nat/2009/09-h065e.htm> >.

that security awareness programs be offered at airports,¹⁹⁶⁹ as well as various ways of controlling access to restricted areas.¹⁹⁷⁰

As is the case with air cargo security, Transport Canada has known about shortcomings in airport security for over two decades.¹⁹⁷¹ Unlike the case with air cargo security, there have been significant improvements in protecting the airport environment. However, non-passengers and others with access to non-public areas of the airport continue to pose an unacceptable risk. Security improvements have not fully addressed this risk.

3.8.2.2 Basic Principles

As some aviation security experts who appeared before the Commission noted, security begins on the ground. Once a plane is airborne, there are only limited means to address a security threat.¹⁹⁷² This may seem self-evident, but it cannot be overstated. The “ground” is the airport, where security measures must be implemented and maintained in a coordinated, mutually reinforcing manner. Complementary layers of security are necessary.¹⁹⁷³ In his 1993 book, *Combating Air Terrorism*, Wallis wrote of the important role of the airport in preventing air terrorism:

Any incident of unlawful interference has its origins on the ground. To sabotage or hijack an aircraft requires security defences in place at airports to be breached. For this reason much of the Security Annex to the Chicago Convention on Civil Aviation (Annex 17) concentrates on the airport and on the ground procedures considered necessary to preempt criminal acts against civil aviation. It is important to note that the annex defines the minimum criteria required.

The 1985 incidents involving the seizure of the TWA Boeing 727 and the destruction of Air India’s Boeing 747 concentrated the world’s attention on the security provisions at international airports. More specifically, focus was given to identifiable inadequacies.¹⁹⁷⁴

To be fully effective, airport security requires the coordinated efforts of many aviation stakeholders, including Transport Canada, the airport operator, CATSA,

¹⁹⁶⁹ See, for example, Exhibit P-169, p. 58 of 202.

¹⁹⁷⁰ See, for example, Exhibit P-169, p. 69 of 202.

¹⁹⁷¹ Exhibit P-101 CAF0695.

¹⁹⁷² Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 4999-5000; see also Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4940.

¹⁹⁷³ Testimony of Jim Marriott, vol. 39, June 4, 2007, p. 4708.

¹⁹⁷⁴ Wallis, *Combating Air Terrorism*, p. 44. The seizure of TWA Flight 847 by Lebanese Hezbollah terrorists on June 14, 1985, occurred over the Mediterranean. It was a two-week hostage-taking in which the hijackers negotiated for the successful release of hundreds of prisoners in Lebanon and Palestine. See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

air carriers and local police. Consultation with all those affected and involved in the development and implementation of airport security measures will result in optimal security.¹⁹⁷⁵

3.8.2.3 Air Terminals as Targets of Opportunity

Air terminals themselves are targets. Long line-ups and passenger congestion at check-in and security counters mean that many people are assembled in a confined area, creating a target-rich environment.¹⁹⁷⁶ As well, a security breach that sees passengers evacuated from secure areas creates congestion in non-secure areas and provides a target of opportunity.¹⁹⁷⁷ This was the concern in August 2006 at London's Heathrow Airport, when authorities uncovered a plot to hide liquid and gel explosives in hand baggage. The rapid security response resulted in "absolute chaos"¹⁹⁷⁸ at the airport, as large groups of passengers were made to gather in tents outside the airport. Wallis testified that "...[t]his is the sort of knee-jerk reaction we have to avoid because the moment you bring them all out into the open, you've created a massive target if the terrorists were serious."¹⁹⁷⁹

Many experts view aircraft sabotage as holding the greatest appeal for terrorists¹⁹⁸⁰ since aircraft can be clearly identified as surrogates for the state under whose flag they fly,¹⁹⁸¹ and their dramatic destruction in mid-air may provide high propaganda returns.¹⁹⁸² Airports themselves have nonetheless become significant targets since aviation terrorism became more prevalent in the mid-1960s.¹⁹⁸³ An attack in an air terminal building no doubt sends a powerful message to the country in which it is situated.¹⁹⁸⁴ Several significant airport attacks have occurred:

- 1965: Seven British children were injured when a grenade was thrown at the Aden airport terminal in Yemen;
- 1972: In what is referred to as the "Lod Airport Massacre," the Popular Front for the Liberation of Palestine (PFLP) and Japanese Red Army terrorists opened fire in the passenger terminal of Lod (renamed Ben-Gurion) Airport in Israel, killing 26 and wounding 78;
- 1973: A Black September suicide squad attacked the passenger terminals at Athens Airport in Greece, killing 3 and injuring 55;
- 1973: Palestinian terrorists bombed a Pan Am office at Fiumicino Airport in Rome, Italy, killing 32 and injuring 50;

¹⁹⁷⁵ Wallis, *Combating Air Terrorism*, p. 52; see also Exhibit P-169, p. 49 of 202.

¹⁹⁷⁶ Exhibit P-169, p. 57 of 202.

¹⁹⁷⁷ Exhibit P-169, p. 57 of 202.

¹⁹⁷⁸ Testimony of Peter St. John, vol. 37, May 31, 2007, p. 4510.

¹⁹⁷⁹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4248.

¹⁹⁸⁰ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4243; see also Exhibit P-169, p. 15 of 202.

¹⁹⁸¹ Wallis, *Lockerbie*, p. 152.

¹⁹⁸² Exhibit P-169, p. 15 of 202.

¹⁹⁸³ Exhibit P-35, p. 18.

¹⁹⁸⁴ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4244.

- 1975: Arab terrorists attacked Orly Airport in Paris, France, seizing 10 hostages in a terminal bathroom;
- 1975: A bomb was detonated at LaGuardia Airport in New York, killing 11 and injuring 74;
- 1976: PFLP and Japanese Red Army terrorists attacked a passenger terminal at Istanbul airport in Turkey, killing 4 and injuring 20;
- 1985: A Red Army Faction bomb exploded at Frankfurt Airport, Germany, killing 3; and
- 1985: Using grenades and machine guns, the Abu Nidal terrorist group launched suicide attacks on passenger terminals at both Rome and Vienna airports, killing 16 and injuring more than 100.¹⁹⁸⁵

The 1985 attacks at Rome and Vienna Airports targeted the check-in operations of the Israeli air carrier, El Al. The attacks signalled the onset of a new phenomenon – the “disposable” terrorist. Whether the attacks were intended to be suicidal is disputed,¹⁹⁸⁶ since the terrorists attempted to escape, but “[t]he absence of a coordinated, preplanned escape avenue suggests that the planners behind the attacks were content to have their forces disposed of after the event.”¹⁹⁸⁷ In other words, the planners appeared not to be concerned if attackers were killed or captured during their attack.¹⁹⁸⁸

The Rome and Vienna airport attacks led the International Civil Aviation Organization (ICAO) ¹⁹⁸⁹ to develop a protocol to the *Montreal Convention*, the international treaty dealing with sabotage against aircraft. The treaty had not envisaged attacks on air terminals. On February 24, 1988, the protocol was finalized. It declared as an offence any act of violence against persons, facilities or services at an international airport that could cause serious injury, death or damage, as well as the destruction or damage of aircraft not in service at such airports.¹⁹⁹⁰

There has been a relative lull in attacks on airport terminals since the 1985 Rome and Vienna incidents.¹⁹⁹¹ However, it stands to reason that, as security defences to safeguard aircraft – for example, passenger and baggage screening – are

¹⁹⁸⁵ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁹⁸⁶ According to Rodney Wallis, the terrorists had not planned to “fight to the death” – the usual expectation of suicide missions. See Wallis, *Combating Air Terrorism*, p. 11.

¹⁹⁸⁷ Wallis, *Combating Air Terrorism*, p. 11.

¹⁹⁸⁸ Wallis, *Combating Air Terrorism*, p. 11.

¹⁹⁸⁹ Established in 1944, ICAO is the supreme law-making body for international civil aviation. See Wallis, *Combating Air Terrorism*, p. 91.

¹⁹⁹⁰ Wallis noted that the necessity for such an international protocol to the original Montreal Convention can be questioned since armed attacks involving injury and death would invariably be addressed by national criminal statutes. However, by linking such crimes to the Montreal Convention, states were afforded the opportunity to extradite the offenders to the country against which the crime was targeted. See Wallis, *Combating Air Terrorism*, p. 12.

¹⁹⁹¹ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

strengthened, terrorists will turn to other targets.¹⁹⁹² The airport terminal is one such target.¹⁹⁹³

Since 2000, there have been further incidents of sabotage at airport terminals and there are fears of more. In 2003, a bomb hidden in a backpack exploded in the terminal in Davao, in southern Philippines, killing 21 people and wounding 148. The Moro Islamic Liberation Front was suspected.¹⁹⁹⁴ Immediately following the events of September 11th, one of the main concerns in the US was the vulnerability of airport terminals. The US was particularly concerned about the ease with which vehicles could gain access to the front entrance of airports and the potential for an explosives-laden vehicle to drive up to the air terminal and be blown up. A decision was made to close airport parking within 100 yards of the front of terminal buildings. Airport industry trade associations objected because of the significant lost income from the closed parking spots. The industry rejected the option of searching every vehicle, also because of the cost. The parking spots were nevertheless closed but, according to Moses Aléman, a US-based expert in international civil aviation security, concern later appeared to subside and the vehicle ban was lifted.¹⁹⁹⁵

Complacency and industry concern over lost revenue appeared to play a role in discontinuing this security measure. Wallis identified complacency as an ongoing problem:

Complacency is an ever-present problem.... [I]f you go a period without anything happening complacency sets in. It can set in with an airline, with an airport or with governments.

Governments don't continue with their initial big push on changes in legislation, for example, if nothing has been happening. They have got other things, other sound bytes they want to put up to push the current political thinking, et cetera.¹⁹⁹⁶

Wallis strongly emphasized that cost issues must not take priority over security: "...[C]ommercial priorities, namely bottom-line figures in the company accounts, must not be allowed to override security requirements."¹⁹⁹⁷ He quoted Victoria Cummock, a disaster victims advocate whose husband was on board Pan Am Flight 103 and died when it was bombed in 1988. She stated that "...history has proven the aviation industry's lack of sincerity and willingness to address safety

¹⁹⁹² Exhibit P-361, Tab 1, p. 8.

¹⁹⁹³ Exhibit P-169, p. 57 of 202.

¹⁹⁹⁴ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

¹⁹⁹⁵ Testimony of Moses Aléman, vol. 35, May 29, 2007, pp. 4245-4246.

¹⁹⁹⁶ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4541.

¹⁹⁹⁷ Wallis, *How Safe Are Our Skies?*, p. 167.

and security on behalf of their customers.” Wallis insisted that such an attitude must not be allowed to persist in the 21st century.¹⁹⁹⁸

The very event feared by the US recently came to pass, albeit in Scotland. On June 30, 2007, a sports utility vehicle filled with gas canisters was deliberately driven through the front doors of the main terminal building at Glasgow Airport and set ablaze.¹⁹⁹⁹

Although risks must be assessed in their local context, a proactive approach to security requires an ongoing assessment of trends in aviation terrorism, wherever they occur. Good risk management principles dictate that significant risks be reduced to a level that is considered acceptable, given available resources.²⁰⁰⁰ When the Commission asked whether the Canadian Airports Council (CAC) had attempted to address the risk presented by target-rich airport environments, it was told of the many difficulties in determining risk priorities:

...[W]e’re confronted with a broad variety of security threats and the challenge for Transport Canada, from our perspective, and the challenge for our [security] committee and our members, is to identify those risks that are the highest potential, the ones that are the most urgently demanding of our attention from a security perspective.

So with each event that occurs it highlights an issue that calls for an answer from the aviation community but the challenge is identifying the risk of that event ever happening again, how to decide whether that is one that’s likely to be exploited again and how to respond in a measured way by the...aviation stakeholders.²⁰⁰¹

Managing the totality of security risks presents challenges, but adherence to a common set of risk management protocols based on best practices in the field, coupled with ongoing consultation with all relevant stakeholders, will lead to robust aviation security.²⁰⁰²

Several potential solutions may exist for each security weakness. Not all measures will be practical in all settings. For example, closing off the front of a terminal

¹⁹⁹⁸ Wallis, *How Safe Are Our Skies?*, p. 168.

¹⁹⁹⁹ Exhibit P-425, pp. 1-2 of 5.

²⁰⁰⁰ “Good risk management practices dictate that, so far as risk control objectives are concerned, *there must be no gaps in the system*: The whole set of risk domains must be managed so as to achieve performance outcomes according to a predetermined level of acceptable risk. If this cannot be accomplished in any one domain, either risk control resources must be rebalanced across those domains, or additional resources must be allocated.” [Emphasis in original] See Exhibit P-361, Tab 1, p. 9.

²⁰⁰¹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8122.

²⁰⁰² Exhibit P-361, Tab 1, pp. 8-10; see also Section 3.3, which describes risk management in civil aviation security.

building to vehicles, though likely to enhance security, may be unworkable, a reality that seems to have been recognized by US authorities. It is a long-established principle that security measures must not unreasonably impede air travel.²⁰⁰³ However, industry concerns must not block necessary security measures. A well-considered balance between security and industry needs is necessary. Jean Barrette, Director of Security Operations at Transport Canada, discussed how security and other considerations are weighed:

In anything we do in security, we always look at the triangle, as I call it. Security ... is your ultimate objective.... [W]e have to create an environment commensurate to good business; that's the business that our colleagues in the air carrier industry are in. And ... keeping in mind the rights and the values of our Canadian citizens.... [W]hen you are facing a security situation ... [the] impact on the business of the air carrier, that is no relevancy to us because what comes first is our engagement to make sure we ensure the safety and security of passengers.

... [W]e are in the business of preventing acts of unlawful interference and the security of the passengers will also have precedence over business.²⁰⁰⁴

The Commission heard of possible solutions as drastic as redesigning air terminal buildings. Other solutions could involve security measures to reduce the number of passengers congregating in any one area.²⁰⁰⁵ Airport authorities in some countries prohibit anyone other than passengers from entering the terminal building.²⁰⁰⁶ Airport security committees also need to reassess emergency evacuation procedures to avoid large crowds gathering in non-secure areas.²⁰⁰⁷

3.8.2.4 The Price of Poor Access Control

Access control, perimeter security and facilities protection are vital to airport security and can directly affect aircraft – and therefore passenger – security.²⁰⁰⁸ The CATSA Act Review Advisory Panel (CATSA Advisory Panel), an independent advisory panel, agreed in a 2006 report that access to restricted areas and airside portions of the airport "... through air terminal buildings, from the ramp or apron where aircraft are loaded, through the outer perimeter that encloses the wider airfield, through airfield gates or tenant facilities, on foot or in a

²⁰⁰³ The 1985 Seaborn Report recognized that "...[t]he threat of terrorism must not be permitted unduly to interfere with the normal activities of daily life, including air travel." The report recognized, as well, that air travellers are susceptible to terrorism and that security must therefore be efficient and effective. See Exhibit P-101 CAF0039, p. 10 of 10.

²⁰⁰⁴ Testimony of Jean Barrette, vol. 38, June 1, 2007, p. 4567.

²⁰⁰⁵ Exhibit P-169, p. 57 of 202.

²⁰⁰⁶ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4244.

²⁰⁰⁷ Exhibit P-169, p. 57 of 202.

²⁰⁰⁸ Wallis, *How Safe Are Our Skies?*, p. 87.

vehicle – must be rigorously secured at all times.”²⁰⁰⁹ All operational areas of the airport, particularly the ramp, must be protected from terrorist infiltration. The ramp, which forms part of the airport tarmac, has been described as the “soft underbelly of an airport.”²⁰¹⁰ It is the area immediately beside the terminal building where most aircraft park.²⁰¹¹ With increasingly large aircraft that require more vehicles, equipment and personnel to service them, it becomes difficult to maintain tight security controls around the aircraft²⁰¹²:

Movement around an aircraft being prepared for flight is very confused. A multitude of vehicles are used to service the aircraft while a myriad of staff are needed for the same purpose. Engineers, caterers, cleaners, and refuelers, together with persons emptying the waste tanks, are all at or around the aircraft at some time during its period on the ramp. This confused mass of staff can be used to cloak the activity of a terrorist, or someone aiding him, to position an explosive device or weapons onto an aircraft. Experience has shown that this approach has been used many times to provision terrorists who have been able to walk cleanly through airport controls only to collect their weapons once they are on board.²⁰¹³

Terrorists have exploited inadequate airport security controls to attack aircraft on the ground:

- 1968: The PFLP launched a machine gun attack on an El Al aircraft at the airport in Athens, Greece, killing 1;
- 1969: Using machine guns, Palestinian terrorists attacked an El Al 707 on the runway in Zurich, Switzerland, raking the fuselage with gunfire and killing the pilot and 3 passengers; and
- 1986: Terrorists breached perimeter security at Karachi Airport in Pakistan and seized a Pan American 747 that was in the process of boarding, killing 22 and injuring more than 100.²⁰¹⁴

The 1986 incident at Karachi Airport involved terrorists dressed to resemble airport guards. They obtained a vehicle similar to those used by the airport authority and drove to a checkpoint at the entrance to the airside of the airport. Despite security rules that required identity cards to be examined, the terrorists were simply waved through, giving them unimpeded access to the aircraft.²⁰¹⁵

²⁰⁰⁹ Exhibit P-169, p. 58 of 202.

²⁰¹⁰ Wallis, *How Safe Are Our Skies?*, p. 77.

²⁰¹¹ Wallis, *How Safe Are Our Skies?*, p. 77.

²⁰¹² Wallis, *How Safe Are Our Skies?*, pp. 70-71.

²⁰¹³ Wallis, *Combating Air Terrorism*, p. 59.

²⁰¹⁴ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

²⁰¹⁵ Wallis, *How Safe Are Our Skies?*, p. 87.

The likelihood of a similar attack in Canada may seem remote. However, Canada's experience with air terrorism and the identification of perimeter security as a key concern in 1985 following the bombing of Air India Flight 182, and a recent occurrence at Toronto's Pearson International Airport, suggest the need for greater concern. According to media reports, Senator Colin Kenny, Chair of the Senate Committee, accompanied by the Minister of Transport, the Hon. John Baird, staged an undercover incursion at Pearson International Airport on March 29, 2009, following months of planning. They drove to the perimeter of the airport in a police van, stepped out of the vehicle and quickly found an unguarded entranceway through which they passed, unchallenged. They then spent time wandering about the airport tarmac, mingling with airport workers. Both intruders wore baseball caps and the Senator had donned "an orange traffic vest and made a show of carrying around a clipboard, and an array of ID cards and hotel room keys, none of which were related to airport security."²⁰¹⁶ Although they spoke with airport workers, including fuellers and baggage handlers, their presence on the tarmac, a restricted area, was never questioned. The Greater Toronto Airports Authority (GTAA) had evidently provided the pair with appropriate visitor passes, but these went unchecked and they were never asked to leave the area. Senator Kenny was said to have claimed that the passes were "irrelevant for getting on the tarmac."²⁰¹⁷

The impromptu "intrusion test" staged by Senator Kenny and Minister Baird in many ways mirrored the methods used by terrorists in the Karachi Airport incident in 1986.

Six months before this incursion, the Commission heard from the Director of Public Safety at the GTAA. He explained the approach to perimeter security at Pearson International Airport:

We have a tiered response for all our securities to, in essence, put the right people at the right place at the right time. In perimeter security what that means is that everyone who is on the airfield is responsible for the perimeter checks. So our standards, just by the nature of who we are, are higher than the standards that Transport Canada set.

That was our choice. Our checks are more frequent so it's not only security that does perimeter checks. [Canine teams do] security checks. The field operations group does security checks, airside safety, and it's a random checking of the

²⁰¹⁶ Colin Freeze, "Operation Tarmac: politicians go undercover to expose security flaws at Pearson" *The Globe and Mail* (2 April 2009), online: <<http://web.theglobeandmail.com/servlet/story/LAC.20090402.KENNY02/TPStory/National>>.

²⁰¹⁷ According to the media reports, Senator Kenny and Minister Baird were followed throughout by RCMP officers, who had briefed the pair prior to the incursion, but did not direct their wanderings on the airport tarmac. See Colin Freeze, "Operation Tarmac: politicians go undercover to expose security flaws at Pearson" *The Globe and Mail* (2 April 2009), online: <<http://web.theglobeandmail.com/servlet/story/LAC.20090402.KENNY02/TPStory/National>>.

perimeter for obviously holes in the fence but also tire marks and people hanging around and that sort of thing.²⁰¹⁸

The CATSA Advisory Panel conceded that security can never be absolute, but that it must be brought to an acceptable level, based on relative levels of risk.²⁰¹⁹

In his book, Wallis wrote of a series of incidents between 1998 and 2000 where stowaways were discovered in the nose wheel bay and undercarriage of aircraft belonging to British Airways, upon their return to the United Kingdom from abroad. Although Wallis stated that none of the stowaways had threatened the security of the aircraft, their presence revealed a serious security loophole:

If it is possible for would-be refugees to access an aircraft undetected, what of terrorists who could so easily plant an improvised explosive device in this very vulnerable position? A timing mechanism could be set to detonate a device at any point in the aircraft's flight, including over a major metropolis.²⁰²⁰

An airport's defence must provide protection against a wide range of potential attackers.²⁰²¹ Terrorists can sometimes pretend to be legitimate employees, or legitimate employees can be "turned" to act as terrorists. For this reason, access to restricted and airside areas of the airport must be effectively controlled.²⁰²² Non-passengers include employees of airports, airlines, CATSA, government agencies, retailers and restaurants, as well as service providers under contract to any of these entities.²⁰²³ As noted earlier, the ramp represents a key vulnerability:

When aircraft arrive or are preparing for departure, the ramp is a hive of activity. The larger the aircraft, the more airport workers and service vehicles need access to the area. All have to be security screened and supervised. The aircraft has to be guarded against unauthorized entry.²⁰²⁴

The history of air terrorism has shown the risk posed by workers with access privileges at airports. The earliest suspected case occurred in 1955 and involved the bombing of an Air India Lockheed 749A. A bomb exploded while the aircraft flew over the South China Sea. Only three of the 19 persons on board survived. The flight originated in Hong Kong and was carrying Chinese delegates and journalists to a conference in Indonesia. A Chinese aircraft cleaner had

²⁰¹⁸ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8130-8131.

²⁰¹⁹ Exhibit P-169, p. 36 of 202; see also Section 3.3, which describes in greater detail risk management in civil aviation security.

²⁰²⁰ Wallis, *How Safe Are Our Skies?*, p. 89.

²⁰²¹ Wallis, *Combating Air Terrorism*, p. 51.

²⁰²² Wallis, *How Safe Are Our Skies?*, p. 91.

²⁰²³ Exhibit P-169, p. 67 of 202.

²⁰²⁴ Wallis, *How Safe Are Our Skies?*, p. 77.

reportedly been bribed to place an incendiary device in the starboard wheel well. This illustrates how an airport worker can be used to aid in the sabotage of an aircraft. Political terrorism was the apparent motive. The Chinese Premier may have been the target, but his travel plans had been kept secret and he flew three days later.²⁰²⁵

In 1986, a bomb exploded on an Air Lanka Lockheed 1011 aircraft while it was on the ground at Colombo Airport, killing more than 20 passengers who were boarding the aircraft. A customs officer with access to the aircraft's supplies and who was believed to be sympathetic to the Tamil separatist movement was charged with sabotage. The device had been placed in the aircraft's "fly-away" kit, a collection of essential technical items carried on each aircraft to facilitate emergency maintenance at overseas airports.²⁰²⁶ In December 1987, a dismissed US Air employee with a grudge against his former supervisor and the company boarded a US Air aircraft in Los Angeles. He had retained his airline identification badge, which permitted access to the airside of the airport. He reached the aircraft simply by walking around the screening controls. He was known to the screeners, who apparently did not know that he had been fired. He is believed to have used a smuggled revolver to kill his former supervisor and then the flight deck crew, causing the aircraft to crash. All 43 persons on board were killed.²⁰²⁷

The bombing of Pan Am Flight 103 in December 1988 was initiated by a breach in airside security involving a former airline security executive. The suitcase containing the bomb had circumvented regular check-in procedures because the perpetrator, a former chief of security with Libyan Arab Airlines,²⁰²⁸ had links to the airline. This gave him access to the baggage makeup area at the airport in Malta and, ultimately, to the baggage tags. The suitcase was labelled with an interline tag,²⁰²⁹ placed aboard the Air Malta aircraft and later interlined to the Pan Am flight in Frankfurt. Following a transit stop and change of aircraft at Heathrow Airport in London, the bomb exploded while over Lockerbie, Scotland. All 259 people on board died, along with 11 people on the ground killed by the aircraft's debris.²⁰³⁰

As these aviation security incidents demonstrate, stringent airport access control, including perimeter security, is essential. Only individuals and vehicles with authorization to enter restricted areas or airside portions of airports should be allowed to do so.²⁰³¹ Still, as history has shown, even those who are considered known and trusted can harm civil aviation.

²⁰²⁵ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

²⁰²⁶ See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

²⁰²⁷ Wallis, *Combating Air Terrorism*, p. 51.

²⁰²⁸ The perpetrator was also an intelligence officer of the Libyan government. In 2001, he was found guilty of murder in the bombing of Pan Am Flight 103 and was sentenced to 27 years in prison: Wallis, *Combating Air Terrorism*, p. 38.

²⁰²⁹ Testimony of Rodney Wallis, vol. 37, May 31, 2007, p. 4516.

²⁰³⁰ See Section 2.3, which provides a detailed analysis of the bombing of Pan Am Flight 103.

²⁰³¹ Wallis, *How Safe Are Our Skies?*, p. 156.

3.8.2.5 Access Control at Canadian Airports

Despite a recognized need for robust airport security, and despite the measures already implemented to improve protection of the airport environment, many witnesses told the Commission that access control at Canadian airports was one of the key security deficiencies in civil aviation.²⁰³² Inadequate screening of non-passengers and weak perimeter security were the main concerns.²⁰³³ In 2006, the CATSA Advisory Panel completed a review of CATSA's operations and enabling legislation. The Panel expressed concern about how easily unauthorized individuals could enter restricted areas of airports, labelling this a "major lacuna"²⁰³⁴ in Canada's defence against air terrorism. Reports by the Senate Committee²⁰³⁵ and the Auditor General of Canada²⁰³⁶ largely agreed.

The CATSA Advisory Panel found unauthorized access to be a particularly acute problem at larger airports, where tens of thousands of long-term, temporary and casual workers were employed. These included baggage handlers, plane groomers and employees of catering, cargo and retail establishments.²⁰³⁷ At Canada's busiest airport, Pearson International Airport in Toronto, more than 45,000 employees had legitimate access to restricted areas.²⁰³⁸

Many areas at major airports were reportedly unguarded, or open for individuals to roam without challenge or any form of screening. These included such critical areas as the tarmac, aircraft hangars, catering facilities and the airport perimeter.²⁰³⁹ Vehicles that entered the perimeter were not searched.²⁰⁴⁰ Although it provided anecdotal evidence only, the undercover intrusion conducted by Senator Kenny and Minister Baird at Pearson International Airport exposed some of these serious security weaknesses.²⁰⁴¹ The Commission is troubled by these reports.

These criticisms of airport security echo concerns that were identified as early as 1985 and repeated when measures were introduced to improve access control after September 11th. On November 5, 2002, CATSA, then a newly created screening authority, became responsible for the random screening of non-passengers who sought access to restricted areas at airports, as well as random screening of their possessions.²⁰⁴² CATSA was also given responsibility for developing the Restricted Area Identification Card (RAIC), which used

²⁰³² See, for example, Exhibit P-169, pp. 57-58 of 202.

²⁰³³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4626; see also Exhibit P-169, pp. 57-58 of 202.

²⁰³⁴ Exhibit P-169, p. 58 of 202.

²⁰³⁵ Exhibit P-172, p. 28 of 155.

²⁰³⁶ Exhibit P-173, p. 4.

²⁰³⁷ Exhibit P-169, p. 58 of 202.

²⁰³⁸ Exhibit P-169, p. 31 of 202.

²⁰³⁹ Exhibit P-169, p. 58 of 202.

²⁰⁴⁰ Exhibit P-172, pp. 30 and 32 of 155.

²⁰⁴¹ Colin Freeze, "Operation Tarmac: politicians go undercover to expose security flaws at Pearson" *The Globe and Mail* (April 2, 2009), online: *The Globe and Mail* < <http://web.theglobeandmail.com/servlet/story/LAC.20090402.KENNY02/TPStory/National> >.

²⁰⁴² Exhibit P-169, p. 61 of 202; see also Final Submissions of the Attorney General of Canada, Vol. II, para. 373.

biometric identifiers to augment and replace the existing Restricted Area Pass (RAP) system.²⁰⁴³ Non-passenger screening (NPS) is now conducted randomly at either temporary or permanent locations established at entry points to restricted areas. NPS activities are currently focused on restricted area access points in air terminal buildings, where employee traffic is reportedly higher.²⁰⁴⁴ At the largest Class 1 airports, CATSA uses a combination of permanent NPS checkpoints and “roving” teams of screeners that move between various access points “to increase the unpredictability of the program.”²⁰⁴⁵ By 2006, six permanent NPS locations at Class 1 airports across Canada were equipped with walk-through metal detectors.²⁰⁴⁶ This meant that the majority of doors giving access to restricted areas did not have a fixed NPS checkpoint. Rather, the NPS team used a mobile cart that included hand-held metal detectors and moved on a random basis between access points where there was no fixed metal detector.²⁰⁴⁷ Items carried by non-passengers might be checked with X-ray and/or explosives detection trace (EDT) equipment. Secondary searches might be conducted to check suspect items. Any non-passenger who refused a search was denied entry to the restricted area.²⁰⁴⁸ The Commission had no information about the number of permanent NPS locations in place at the time of writing.

Perimeter security is the responsibility of the airport operator.²⁰⁴⁹ In its Final Submissions, the Attorney General of Canada reported that vehicles “...are subject to only cursory, visual examination by airport operators at a limited number of vehicle access gates.”²⁰⁵⁰ At present, CATSA screening officers do not search vehicles when they enter a restricted area.²⁰⁵¹ However, in July 2006 Transport Canada reported to the Senate Committee that it was working with CATSA on “implementation strategies for vehicle searches.”²⁰⁵² The Attorney General’s Final Submissions also reported that Transport Canada and CATSA were cooperating to develop options to improve NPS and to conduct vehicle searches at Class 1 airports.²⁰⁵³

NPS procedures were implemented requiring CATSA to screen non-passengers and their possessions on a random basis before allowing entry to restricted areas²⁰⁵⁴ in the 29 Class 1 and Class 2 airports,²⁰⁵⁵ but faced much criticism. There was widespread agreement about the need for NPS, but also concern that random screening would inescapably miss many individuals, including some

²⁰⁴³ Exhibit P-169, p. 73 of 202; see also Exhibit P-101 CAF0858, p. 1 of 10.

²⁰⁴⁴ Exhibit P-273, p. 34; see also Final Submissions of the Attorney General of Canada, Vol. II, para. 377.

²⁰⁴⁵ Final Submissions of the Attorney General of Canada, Vol. II, para. 377; see also Exhibit P-169, p. 67 of 202.

²⁰⁴⁶ The six permanent NPS checkpoints were reported to be located in Calgary (2), Halifax (1), Winnipeg (2) and Edmonton (1). See Exhibit P-172, p. 32 of 155; see also Exhibit P-173, p. 34.

²⁰⁴⁷ Exhibit P-173, p. 34.

²⁰⁴⁸ Exhibit P-169, pp. 67-68 of 202.

²⁰⁴⁹ Exhibit P-169, p. 57 of 202.

²⁰⁵⁰ Final Submissions of the Attorney General of Canada, Vol. II, para. 380.

²⁰⁵¹ Exhibit P-169, pp. 67-68 of 202.

²⁰⁵² Exhibit P-172, p. 32 of 155.

²⁰⁵³ Final Submissions of the Attorney General of Canada, Vol. II, para. 382.

²⁰⁵⁴ Exhibit P-169, p. 67 of 202.

²⁰⁵⁵ Exhibit P-173, p. 10.

with ill intentions. For some, this weakness called the effectiveness of the overall NPS program into question.

In its 2007 report on airport security in Canada, the Senate Committee concluded that random screening of non-passengers effectively translated into “seldom” screening.²⁰⁵⁶ Transport Canada reported in 2006 that about 2,300 airport workers were screened each day at 89 airports across Canada. However, the Senate Committee heard evidence suggesting that only about half that number, or about 1,200 workers a day, were being screened out of a total of about 100,000.²⁰⁵⁷ The Committee observed that this amounted to “little more than 1 percent of non-passengers entering restricted areas.”²⁰⁵⁸ The Commission notes that even Transport Canada’s higher estimate that 2,300 workers were screened daily covers a surprisingly low percentage of those who have access to restricted areas of airports.

The Senate Committee also heard disturbing evidence about how employees avoided the screening process altogether, such as by using cellphones to warn others of an NPS check.²⁰⁵⁹ As well, the NPS program did not operate around the clock. In 2006, Transport Canada informed the Committee that the hours of operation for CATSA’s NPS program were to be increased “...[i]n order to increase the level of service.”²⁰⁶⁰ Even so, NPS services were not available 24 hours a day. The Committee suggested that non-passengers could circumvent the screening process by waiting to access a restricted area during times when NPS was not operating.²⁰⁶¹ In Final Submissions to the Commission in 2008, the Attorney General of Canada reported that NPS coverage at the eight Class 1 airports was generally 16 to 20 hours per day.²⁰⁶² Choosing to enter during hours when there was no coverage would avoid even the remote possibility of being caught by random screening. The Senate Committee concluded that there was no assurance that random checks were anything but infrequent, and no assurance that canny employees could not avoid checks altogether.²⁰⁶³ Of all problems with airport security identified by the Senate Committee, NPS was its primary concern: “...If there was one thing that...the Committee could fix tomorrow, it would be non-passenger screening.”²⁰⁶⁴

In its 2006 Special Examination Report of CATSA, the Auditor General of Canada similarly singled out NPS as requiring improvement:

Non-passenger screening is another area of concern. Security measures require CATSA to screen non-passengers randomly

²⁰⁵⁶ Exhibit P-172, p. 28 of 155.

²⁰⁵⁷ Exhibit P-172, p. 39 of 155.

²⁰⁵⁸ Exhibit P-172, p. 33 of 155.

²⁰⁵⁹ Exhibit P-172, p. 33 of 155.

²⁰⁶⁰ Exhibit P-172, p. 31 of 155.

²⁰⁶¹ Exhibit P-172, p. 33 of 155.

²⁰⁶² Final Submissions of the Attorney General of Canada, Vol. II, para. 376.

²⁰⁶³ Exhibit P-172, p. 33 of 155.

²⁰⁶⁴ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4687.

at any restricted area access point. CATSA has not conducted screening at restricted area access points outside the air terminal building. The limited number of fixed non-passenger screening check points where random screening occurs and the random nature of the “mobile” non-passenger check points enable the non-passengers to avoid screening.²⁰⁶⁵

To address the concerns raised, the Senate Committee recommended that all individuals and vehicles be screened each time they attempt to enter restricted areas.²⁰⁶⁶ In addition, the Committee recommended random screening of non-passengers when they leave restricted areas (primarily to detect criminal activity, rather than terrorist acts). Each day, at least 10 per cent of those leaving would be screened.²⁰⁶⁷ Currently, no screening occurs when non-passengers leave restricted areas.

Some experts and stakeholders disagreed with 100 per cent NPS. The CATSA Advisory Panel noted that Canada has 89 airports designated for CATSA screening services, which “...range from everything from Pearson in Toronto, which is one of the world’s busiest and largest international airports, to...small places like Iqaluit and Campbell River...which are very, very small operations.”²⁰⁶⁸ Because of this diversity, the Panel objected to a “one-size-fits-all approach to Canadian airports.”²⁰⁶⁹ Instead, it recommended a differentiated approach based on risk. For the largest airports, the Panel recommended “random continuous” NPS, described as follows:

[Random continuous NPS] means that...all points of entry will have controlled access...but that it will be applied on a random basis. So it’s not predictable from the point of view [of] the employees as to whether they’re going to get screened or not and we think that would serve the purpose.²⁰⁷⁰

The Panel recommended that the focus remain on the largest airports – all Class 1 airports, as well as some Class 2 airports as determined on the basis of risk – where the risk is perceived to be greatest.²⁰⁷¹ The Panel explained that, because the busier airports may employ tens of thousands of workers, not all employees know each other. The Panel recommended that random NPS be in place at all times and at all entry points.²⁰⁷² As Chern Heed, one of the Panel

²⁰⁶⁵ Exhibit P-173, p. 10.

²⁰⁶⁶ Exhibit P-172, p. 30 of 155.

²⁰⁶⁷ Exhibit P-172, p. 34 of 155.

²⁰⁶⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4627.

²⁰⁶⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4627.

²⁰⁷⁰ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4627.

²⁰⁷¹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4627.

²⁰⁷² In other words, CATSA would be “continuously present” at all entry points to restricted areas of the airport to perform NPS on a random basis. See Exhibit P-169, p. 69 of 202.

members, testified, this would sufficiently address the risk and reduce NPS staffing requirements:

...[W]hen an airline worker has gone through ten times in that particular day, they [the screeners] sort of know that person by that time and we say that the risk is considerably less in that situation if on seven of those times he goes through without being screened....²⁰⁷³

At smaller airports where there were fewer workers and “everybody knows everybody,” the Panel felt that, once implemented, the RAIC, with its biometric identifiers, would suffice. The Panel concluded that at some smaller airports, adding NPS to the responsibilities of CATSA screeners would be prohibitively expensive.²⁰⁷⁴ The Panel stated that reliance on active security awareness at smaller airports, rather than on NPS, would provide the equivalent level of security.²⁰⁷⁵ The Panel recommended that, once the RAIC with biometric identifiers was in place, NPS be discontinued at Class 2 airports, and implemented only on an as-needed basis in Class 2 and Class Other airports when indicated by a threat analysis.²⁰⁷⁶

Yves Duguay, Director of Security at Air Canada, did not support 100 per cent NPS. He testified that maintaining security at such a high level at all times would encourage complacency, not vigilance, among screeners. Duguay also raised a potential logistical concern – that if, for example, 1,500 employees appeared at the same time for the beginning of a shift at some large airports, this would present challenges for the screening process. Like the CATSA Advisory Panel, Duguay saw continuous random NPS as an additional layer of airport security that would provide sufficient deterrence. He further recommended random screening for non-passengers when they leave restricted areas.²⁰⁷⁷

Wallis described access control as “absolutely vital”²⁰⁷⁸ and insisted that all individuals getting access to restricted areas be security screened and supervised.²⁰⁷⁹ The security of the ramp area, and ultimately the aircraft, demanded this:

The operational area of the airport, the ramp let’s say, has always been the soft underbelly of an airport. You’ve got to protect it. And I don’t believe random screening is acceptable. I think everybody who passes from land side to airside at an airport should be screened. Everybody.²⁰⁸⁰

²⁰⁷³ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4628.

²⁰⁷⁴ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4628.

²⁰⁷⁵ Exhibit P-169, p. 68 of 202.

²⁰⁷⁶ Exhibit P-169, p. 69 of 202.

²⁰⁷⁷ Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5263-5264.

²⁰⁷⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5000.

²⁰⁷⁹ Wallis, *How Safe Are Our Skies?*, p. 77.

²⁰⁸⁰ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5036.

Wallis testified that it would be unwise to exempt employees from screening simply because they are “known.” Such a flawed assumption had devastating results for civil aviation. The customs officer who placed a bomb on an Air Lanka aircraft at Colombo Airport in 1986 is one example. The officer was a person in authority, known to everyone, who had access to the ramp, but who was not screened and who subsequently destroyed an aircraft.²⁰⁸¹ Wallis stated that, had the aircraft been airborne, “...the result would have been as catastrophic as the Air India disaster.”²⁰⁸² In December 1987, as noted, a former US Air employee, known to others at Los Angeles International Airport, was able to bypass security using airline identification that he had not surrendered, and board an aircraft with a loaded gun. While the aircraft was in flight, he shot another passenger, his former supervisor, and then the pilots, sending the aircraft into a fatal dive and leaving 43 people dead.²⁰⁸³ The bombing of Pan Am Flight 103 also involved a former aviation employee – an airline security executive – whose actions resulted in the mid-air destruction of an aircraft that killed 270 people. Some stakeholders have stated that the security background checks conducted before employees are granted access to restricted areas add a protective layer, and that employees who have been vetted through this process should not face screening as extensive as others,²⁰⁸⁴ such as passengers who walk in “off the street” with a ticket and are not known to the system.²⁰⁸⁵

All personnel who require access to restricted areas, whether they are based at a specific airport or travel between airports, such as air crew and maintenance workers, are required to hold a Restricted Area Pass (RAP), as provided by the *Aeronautics Act* and related regulations, measures and orders. Airport authorities issue RAPs, but only to those with a valid security clearance from Transport Canada.²⁰⁸⁶

In its 2003 report on airport security, the Senate Committee found that, too often, passes were not checked, that forgery was a potential problem and that there appeared to be insufficient monitoring to ensure that passes were returned when workers terminated airport employment.²⁰⁸⁷ These were some of the same problems that were identified in the 1985 audit of airport security performed after the bombing of Air India Flight 182.

Although security background checks may bolster confidence in the trustworthiness of airport workers, concerns have remained about the adequacy of the background check process. The Commission learned, for example, that the credit check component of Transport Canada’s security clearance was discontinued in 2006. Yet, as Heed testified, credit checks can identify individuals who might be vulnerable to influence:

²⁰⁸¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5041.

²⁰⁸² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5041.

²⁰⁸³ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5041; see also Wallis, *Combating Air Terrorism*, pp. 2-3.

²⁰⁸⁴ Exhibit P-252, Tab 1, p. 4.

²⁰⁸⁵ Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8150.

²⁰⁸⁶ Exhibit P-169, p. 67 of 202.

²⁰⁸⁷ Exhibit P-171, p. 69 of 256.

...[I]n particular, there is a fair amount of theft that occurs at an airport, and a person's credit history has a lot to do with the chances they'll take if they need the money and [they] could be easily compromised. On that basis, we feel that it's an important indicator of a security risk that person represents.²⁰⁸⁸

This is all the more concerning in light of reports of extensive and increasing organized crime at Canada's airports.²⁰⁸⁹ Organized crime depends on lapses in airport security, preys upon the same human weaknesses that assist terrorist activities and can even have direct ties to terrorism, since some organized crime groups may fund terrorism.²⁰⁹⁰ If thieves and smugglers can exploit security deficiencies, so can terrorists.²⁰⁹¹ A 2008 RCMP report, *Project Spawn*, concluded that 58 organized crime groups were working in or using the eight Class 1 airports for their criminal activities.²⁰⁹² Many in the civil aviation community tend to separate criminal and terrorist activity,²⁰⁹³ but a 2005 independent review of airport security in Australia, known as the Wheeler Report, recognized the possibility of a symbiotic relationship between the two:

Terrorism and crime are distinct, but potentially overlap. At its most basic, a culture of lax security or petty criminality can provide opportunities for terrorists to exploit weaknesses in airport security.²⁰⁹⁴

The RCMP report stated that the main *modus operandi* of organized crime groups at airports is to target airport employees and enlist their aid:

Organized crime groups will attempt to exploit airports by corrupting existing employees or by placing criminal associates into the airport workforce. Criminal networks are known to bribe employees to ignore criminality or to assist in criminal activities, including drug trafficking or theft. The success of organized crime groups at airports depends on their ability to take advantage of security gaps to move contraband without being subject to scrutiny.²⁰⁹⁵

The RCMP report found that some airport employees with RAICs, and who therefore had access to restricted areas, were directly involved in organized

²⁰⁸⁸ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4641.

²⁰⁸⁹ Exhibit P-172, p. 17 of 155; see also Exhibit P-434, p. 12; see also March 2009 Status Report of the Auditor General of Canada, Chapter 1.

²⁰⁹⁰ Exhibit P-172, p. 17 of 155.

²⁰⁹¹ Exhibit P-172, p. 17 of 155.

²⁰⁹² Exhibit P-434, p. 9.

²⁰⁹³ See, for example, Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8140-8141.

²⁰⁹⁴ As quoted from The Independent Review of Airport Security and Policing for the Government of Australia (The Wheeler Report), September 2005. See Exhibit P-169, p. 51 of 202.

²⁰⁹⁵ Exhibit P-434, p. 2.

crime. Almost half of the 298 employees alluded to in its report were implicated in criminal activity at Canadian airports, the majority at the three largest airports. Many had access to some of the most vulnerable areas of the airport:

More than half of the employees in the report worked for ground services companies that work either around airplanes or airport terminals or held positions such as baggage handlers, ramp attendants, cargo handlers, food caterers and aircraft refuellers. These types of jobs give employees extensive access to aircraft and/or luggage, which can be used to smuggle illicit commodities. Other employment sectors include security companies and passenger services companies around the terminal.²⁰⁹⁶

Such individuals can be exploited for terrorist aims as well. As the Wheeler Report stated:

Staff can be bribed to ignore criminality or paid large sums to assist in drug trafficking or theft. Once compromised, such employees may be unable to stand up to terrorists. Any airport staff who are not thoroughly background checked and routinely searched are potential weak links.²⁰⁹⁷

The RCMP report also identified an obvious need for "...vigilance in monitoring employee access to restricted areas and for determining any unusual patterns to that access."²⁰⁹⁸

Despite the illegal activity in the ramp area of airports, a conviction for a criminal offence is not in itself a barrier to a transportation security clearance.²⁰⁹⁹ A 2004 audit by the Auditor General of Canada found that some individuals allowed by Transport Canada to work in restricted areas of airports had criminal records, had been involved in criminal conspiracies or had some association with known criminals.²¹⁰⁰ Transport Canada began to require additional information for reviews of applications for security passes.²¹⁰¹ Even so, a 2009 status report of the Auditor General of Canada referred to the findings of the 2008 RCMP report –

²⁰⁹⁶ Exhibit P-434, p. 15.

²⁰⁹⁷ Exhibit P-434, p. 14.

²⁰⁹⁸ Exhibit P-434, p. 15.

²⁰⁹⁹ Exhibit P-434, p. 16.

²¹⁰⁰ Transport Canada cited the *Aeronautics Act* as limiting its ability to withhold a security pass to situations that relate to "preventing unlawful interference with civil aviation" and that this interference is confined by international convention to activities such as hijacking and sabotage. Although Transport Canada officials agreed that transporting drugs by concealing them in aircraft could be considered unlawful interference, it did not agree that it has a role to play in preventing criminal organizations from infiltrating airports. See March 2009 Status Report of the Auditor General of Canada, Chapter 1.

²¹⁰¹ March 2009 Status Report of the Auditor General of Canada, Chapter 1.

that criminal activity continued to be a significant problem at Canadian airports – and concluded that Transport Canada’s progress was unsatisfactory.²¹⁰²

The Auditor General’s 2009 report noted that the security clearance assessment process was hampered by incomplete information-sharing between the RCMP and Transport Canada. Both unnecessarily withheld important information. The report also criticized Transport Canada for not developing criteria for granting security clearances to individuals with previous criminal links, and for deciding about problematic applications case by case. No criteria differentiated those whose previous offences might indicate a security risk from those whose offences were less serious. One individual granted a pass, for example, had assault and weapons convictions and was under investigation for a murder relating to drug smuggling at a large airport.²¹⁰³

The 2008 RCMP report stated that its ability to determine the extent of criminal infiltration at Canada’s airports was reduced because Transport Canada did not provide information about the percentage of employees with criminal records and the nature of their offences. In particular, information about employees with both RAIC access and criminal records would have assisted the RCMP in its assessment.²¹⁰⁴ The RCMP’s inability to acquire this information, and other concerns about information sharing, are troubling.

Besides criticism about the quality of the security clearance process, the Senate Committee raised concerns about the infrequency of the background checks conducted by Transport Canada once a pass was granted. Checks were conducted every five years. However, concerns about criminality and the possibility of people’s circumstances changing quickly led the Committee to recommend background checks every three years.²¹⁰⁵ The Air Line Pilots Association, International (ALPA) noted, however, that the practice of five-year intervals for background checks was in line with checks of others in sensitive lines of work, such as the RCMP, and that more frequent background checks could place undue strain on a security system that already experienced delays.²¹⁰⁶

The securing of airport perimeters is an essential aspect of aviation security to which Canadian authorities have not paid due attention.²¹⁰⁷ Wallis remarked that:

...[L]ooking at the situation in Canada...[i]f I was to prepare a list of priorities of things to be done, perimeter security with access control would be right at the top of the list....²¹⁰⁸

²¹⁰² March 2009 Status Report of the Auditor General of Canada, Chapter 1.

²¹⁰³ March 2009 Status Report of the Auditor General of Canada, Chapter 1.

²¹⁰⁴ Exhibit P-434, p. 5.

²¹⁰⁵ Exhibit P-172, p. 28 of 155.

²¹⁰⁶ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 7956-7957; Jim Bertram, Director of Public Safety at the GTAA, also noted that the length of time to receive a security clearance is concerning because it can impact security when employees need to work in restricted areas, but have not yet received the appropriate clearance. See Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8141.

²¹⁰⁷ Exhibit P-169, p. 58 of 202.

²¹⁰⁸ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5001.

The searching of vehicles as part of perimeter security is not a CATSA responsibility. Perimeter security as a whole is the responsibility of airport authorities. Fred Jones, Vice President of Operations and Legal Affairs at the CAC, testified that regulations for perimeter security vary from airport to airport according to factors such as their size. Fencing requirements differ, and some smaller airports may not even have fencing. Jones testified that other measures can secure the perimeter, including foot and vehicle patrols and video surveillance. He stated that monitoring perimeter fencing at large airports could present a challenge.²¹⁰⁹

Jim Bertram, Director of Public Safety at the GTAA, cautioned that a full vehicle search could take 10 to 15 minutes. An airport as large as Pearson International Airport may have 5,000 vehicles crossing the perimeter each day. Full searches would lead to significant delays. For this reason, the GTAA supported a risk management-based approach²¹¹⁰ to searching vehicles. Those that were “unknown” were searched, while no search was done of “known” vehicles.²¹¹¹

Wallis acknowledged the challenges faced by larger airports in searching vehicles, but emphasized the importance of having acceptable screening of all vehicles before they are allowed to enter airport premises. It was not sufficient to permit entry simply because an occupant held an RAP:

There is little point in screening workers going onto the airside if you allow them to drive in a vehicle which hasn't been screened or hasn't been subjected to security control.

So you have to check the vehicle. And you've got to look at the operational problems that are going to be associated with this. Having a string of vehicles lined up while somebody is searching them all, you don't want that.²¹¹²

Some vehicles, such as those carrying catering supplies for aircraft, should be security cleared off-airport and appropriately sealed. Any search at the airport perimeter would be limited to the cab of the vehicle.²¹¹³

The objective is always to ensure that dangerous individuals and weapons are prevented from entering airside portions of the airport.

The CATSA Advisory Panel noted that perimeter security, like access control, was recognized as a concern in the 1985 Seaborn Report.²¹¹⁴ This is a continuing weakness that needs to be addressed. The Panel recommended that all vehicles

²¹⁰⁹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8129.

²¹¹⁰ See Section 3.3, which provides a detailed analysis of risk management in civil aviation security.

²¹¹¹ Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8135.

²¹¹² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5037.

²¹¹³ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5037.

²¹¹⁴ Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4640.

entering restricted areas at Class 1 airports be searched by CATSA or under CATSA's oversight, using CATSA standards and procedures.²¹¹⁵ The Panel called for non-passenger and vehicle screening in addition to much more rigorous access control at major airports. In particular, it said that NPS and vehicle screening should be extended to the outer boundaries of Class 1 airports.²¹¹⁶

Wallis strongly advocated for 100 per cent NPS at points of entry to restricted areas. He stated that NPS must remain in place at Class 2 airports where the RAIC system is fully operational because of the need to screen for items brought into restricted areas:

The RAIC will tell you who is where, but it won't tell you who is where with what. In other words, if you have people going into a vulnerable part of the airport, regardless of what ID that they are carrying, they should be screened.²¹¹⁷

Wallis stated that screening non-passengers when they left restricted areas addressed criminal activity such as theft and smuggling. He stated that such screening may well deter such activity where it is a concern, as at many Canadian airports.

Wallis wrote that "...throughout much of the developed world, it had been mandatory for many years for staff, including air crew, to be screened whenever they were airside." As early as 1985, IATA and other international industry associations urged ICAO to make it a firm requirement that all staff be screened in such cases.²¹¹⁸ Annex 17, the security annex to the *Convention on International Civil Aviation* ("*Chicago Convention*"), currently requires screening "a proportion"²¹¹⁹ of non-passengers accessing restricted areas, along with the items they carry. Although the precise proportion is not specified, the security standard provides that this should be determined "in accordance with" a risk assessment.²¹²⁰

According to IATA, no employee group should be granted a blanket waiver from screening. However, rather than calling for a "one-size-fits-all" approach, IATA recommended screening employees by a multi-layered system that reflected their job functions and work sites. The system would rely on thorough employee vetting, deterrence and detection measures designed to minimize opportunities for rogue airport or airline employees to place bombs or other weapons on aircraft or in passenger baggage. IATA emphasized that no stand-alone security process could effectively and reliably screen airline and airport staff. Security

²¹¹⁵ Exhibit P-169, pp. 58 and 69 of 202.

²¹¹⁶ Exhibit P-169, p. 68 of 202.

²¹¹⁷ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5039.

²¹¹⁸ Wallis, *Combating Air Terrorism*, p. 51.

²¹¹⁹ Exhibit P-181, p. 4-1, s. 4.2.6.

²¹²⁰ Exhibit P-181, p. 4-1, s. 4.2.6.

must be multi-layered. IATA also called for non-passenger screening to be based on an appropriate risk assessment.²¹²¹

Some airports abroad have successfully instituted 100 per cent NPS. Major UK airports conduct full NPS, and vehicles entering restricted areas are also screened. The US is also considering extending the partial NPS carried out at large airports to full NPS. Transport Canada must work closely with airports and with CATSA to improve access control through NPS. Full implementation of the RAIC and an enhanced level of security awareness, part of a multi-layered approach to security, will also help.

3.8.2.5.1 Supervision of Non-Security Cleared Individuals

New or short-term employees sometimes work inside restricted areas before their security clearances are processed and a RAP issued. They receive a temporary pass and must be escorted at all times by a RAP holder.²¹²² The Senate Committee saw this as problematic since one “cleared” employee might be responsible for several “non-cleared” workers.²¹²³ The Senate Committee reported that the ratio of “cleared” airport employees escorting or supervising those who are not cleared was as high as one cleared employee for every 10 to 15 non-cleared employees. The Senate Committee called for the ratio to be reduced to one for every five.²¹²⁴ However, Captain Craig Hall, Director of the National Security Committee of ALPA, opposed establishing a firm ratio. For example, if construction workers were working in a confined or fenced-off area, a 1 to 20 ratio might offer sufficient security. However, if a small group was being given a guided tour, a ratio of 1 to 2, or 1 to 1, might be appropriate.²¹²⁵ In every case, appropriate and vigilant supervision of non-security cleared individuals who obtain access to restricted areas must be ensured.

3.8.2.5.2 Restricted Area Identification Card

In November 2002, the Minister of Transport made CATSA responsible for developing and implementing an enhanced pass for restricted areas, the RAIC. The CATSA Advisory Panel concluded that the RAIC would provide effective access control. The RAIC uses biometric identifiers. If a security awareness culture were promoted at the same time, it would complement the implementation of the RAIC.²¹²⁶ Biometrics “authenticate” (provide evidence to prove) a person’s identity by measuring a physical characteristic and comparing that measurement against a template created from the same characteristic.²¹²⁷ The RAIC uses smart card technology, which integrates a small computer chip, including a microprocessor and memory, to store two types of biometric data:

²¹²¹ Exhibit P-258, Tab 1, p. 13.

²¹²² Exhibit P-169, p. 67 of 202.

²¹²³ Exhibit P-171, pp. 67-68 of 256.

²¹²⁴ Exhibit P-172, p. 17 of 155.

²¹²⁵ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7961.

²¹²⁶ Exhibit P-169, p. 58 of 202.

²¹²⁷ Exhibit P-101 CAF0858, p. 1 of 10.

fingerprint and iris templates. The templates are generated by algorithms that encode distinctive features from images of an individual's iris and fingerprint. Significantly, the templates cannot be used to recreate the iris or fingerprint images.²¹²⁸ Transport Canada describes the RAIC as a secure identity card for aviation personnel, including flight crews, those refuelling aircraft, caterers and others needing access to restricted areas at major airports.²¹²⁹ When the program is fully implemented, about 120,000 aviation workers will hold a RAIC.²¹³⁰

The RAIC provides three assurances. It establishes the identity of the RAIC-holder, verifies the cardholder's security clearance and establishes the need and right to be in a particular restricted area. Hall described the RAIC program as one of the foremost in the world.²¹³¹

In its 2006 report, the CATSA Advisory Panel stated that full implementation of the RAIC program had been delayed because resources and a regulatory framework were lacking.²¹³² The Auditor General of Canada concluded that delays in implementing the RAIC system increased risk.²¹³³ The Commission notes that amendments to the *Canadian Aviation Security Regulations* have since introduced provisions about the RAIC program.²¹³⁴

According to the Auditor General's 2006 report on CATSA, the RAIC was deployed and operational in seven Class 2 airports and one Class 1 airport, although not all non-passengers were enrolled. Deployment at the remaining 21 Class 1 and Class 2 airports was ongoing.²¹³⁵ When fully implemented at all 29 Class 1 and Class 2 airports, the RAIC system will have multi-airport capabilities, enabling confirmation of the identity of the holder of an RAIC at any participating airport.²¹³⁶

RAICs are issued by individual airport operators, but are activated by CATSA, which will manage a nationwide identity verification system that can be updated nearly instantaneously and that includes confirmation of an individual's security clearance from Transport Canada. Once notified about a restricted area violation or security clearance infraction, CATSA would deactivate the card, again nearly instantaneously, and the card would no longer be functional.²¹³⁷ Once CATSA completes implementation of the RAIC system, responsibility for operating and maintaining the RAIC system will be transferred to Transport Canada.²¹³⁸

²¹²⁸ Exhibit P-101 CAF0858, p. 2 of 10.

²¹²⁹ Exhibit P-101 CAF0858, p. 1 of 10.

²¹³⁰ Exhibit P-101 CAF0858, p. 2 of 10.

²¹³¹ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 7952.

²¹³² Exhibit P-169, p. 58 of 202.

²¹³³ Exhibit P-173, p. 4.

²¹³⁴ *Canadian Aviation Security Regulations*, SOR/2000-111, ss. 37-53.

²¹³⁵ Exhibit P-173, p. 10.

²¹³⁶ Exhibit P-169, p. 74 of 202.

²¹³⁷ Exhibit P-169, p. 74 of 202.

²¹³⁸ Exhibit P-101 CAF0871, p. 1 of 4.

Individuals receive approval to enter a restricted area by inserting the RAIC into a reader and by providing the biometric required – an iris or fingerprint scan. Individual airport operators may include an access key on the RAIC. If so, the RAIC reader is linked to a point of access to a restricted area. The access point will open once the holder's identity and permission to enter are confirmed. Entry points can be monitored by airport personnel or by automatic double barriers that isolate the individual holding the RAIC while confirmation is in progress. Whether entry points are supervised by airport staff or by mechanical controls, those holding an RAIC will still undergo NPS by CATSA screening officers where they are present at entry points to restricted areas.²¹³⁹

It is also possible to incorporate access keys to multiple airports on a single RAIC. This facilitates movement by aviation personnel, such as flight crews, who require access to restricted areas in many airports for their work. Airport operators have spoken of the need to maintain rigorous access control for restricted areas, but representatives of flight crews stressed the importance of easy, fast and reliable access. The CATSA Advisory Panel was persuaded that the RAIC system would provide the necessary confidence and speed to confirm identities across Canada and that, as a result, it would form the basis for an effective pass for access to several, or all, airports in Canada.²¹⁴⁰ The Panel recommended that the RAIC system be implemented at all designated airports across Canada, not just at the 29 major airports.²¹⁴¹

The Panel recommended further that, once the RAIC system is fully operational, NPS be discontinued at Class 2 airports, and that it be implemented only as needed, based on a threat analysis.²¹⁴² The Panel concluded that in Class Other airports, where employees generally know one another, using the RAIC for electronic entry to secure areas, together with enhanced security awareness, would provide appropriate security. Even so, the Panel recommended that CATSA be prepared to implement NPS in Class 2 and Class Other airports if threat analysis indicates a need.²¹⁴³

The CATSA Advisory Panel noted that the 2006 federal Budget included new funding to extend the RAIC system to Fixed Base Operations (FBOs) in 2006-2007 and to airport perimeters in 2007-2008, once regulatory requirements were in place.²¹⁴⁴

The Senate Committee considered the RAIC alone to be inadequate. It recommended "geo-fencing" in addition.²¹⁴⁵ This would involve passes capable, not only of confirming identity, but also of maintaining a record of the time of each attempt to enter or leave a restricted area. This would enable both tracking of unusual patterns and monitoring of attempts to enter unauthorized areas.

²¹³⁹ Exhibit P-169, p. 74 of 202.

²¹⁴⁰ Exhibit P-169, p. 74 of 202.

²¹⁴¹ Exhibit P-169, p. 75 of 202.

²¹⁴² Exhibit P-169, p. 58 of 202.

²¹⁴³ Exhibit P-169, p. 58 of 202.

²¹⁴⁴ Note: The Commission does not have confirmation that the RAIC has been extended to FBOs or to airport perimeters. Exhibit P-169, p. 58 of 202.

²¹⁴⁵ Exhibit P-172, p. 29 of 155.

Transport Canada reviewed the possibility of a geo-fencing system, but decided that it would produce only limited security gains and therefore decided against it. Barrette testified that geo-fencing could track employees who wear their passes, but not those who removed them.²¹⁴⁶ In 2007, with the RAIC program under way, the Senate Committee called for a planned expansion of the RAIC program to include perimeter security – including vehicle gates, FBOs and tenant facilities – to be implemented more quickly.²¹⁴⁷ The Commission endorses giving priority to expansion of the RAIC program.

3.8.2.5.3 *Instilling a Culture of Security Awareness*

Much airport security is hidden from public view. Access control, including perimeter security, profoundly affects security but largely takes place away from public scrutiny.²¹⁴⁸ Responsibilities in airport security are divided among a number of stakeholders – primarily the airport authority, Transport Canada, CATSA, air carriers and the local police.²¹⁴⁹ For example, CATSA is responsible for screening non-passengers, and the airport operator is responsible for controlling access to restricted areas, including perimeter security, and for issuing RAPs to airport workers.²¹⁵⁰ Because many players are involved in airport security, an effective process to integrate security efforts is needed.²¹⁵¹

In its 2006 report, the CATSA Advisory Panel noted problems in coordinating security activities:

In discussions with the airport authorities and the various police forces, it became evident that there is a lack of clarity, consistency and coordination of aviation security activities. The 2005 *Lessons to be Learned* report, by the Honourable Bob Rae, identifies similar issues from 1985 with respect to the bombing of Air India Flight 182. It is in the interests of all players that airports be secure.²¹⁵²

Several measures can help bring greater consistency and coordination in aviation security, among them a written airport security program and the establishment of an airport security committee, as stipulated by Annex 17 to the *Chicago Convention*.²¹⁵³ A third is security awareness programs.

²¹⁴⁶ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4815.

²¹⁴⁷ Exhibit P-172, p. 39 of 155.

²¹⁴⁸ Wallis, *How Safe Are Our Skies?*, p. 87.

²¹⁴⁹ Exhibit P-169, p. 49 of 202.

²¹⁵⁰ Exhibit P-169, p. 67 of 202.

²¹⁵¹ Exhibit P-169, p. 47 of 202.

²¹⁵² Exhibit P-169, p. 48 of 202.

²¹⁵³ See Section 3.2.2.2.1, which discusses airport security programs and airport security committees in the context of oversight issues in civil aviation security.

Airport Security Watch Program

In the context of aviation security, some describe “culture” as a nebulous term encompassing several initiatives relating to education and awareness and sharing of intelligence.²¹⁵⁴

Transport Canada is moving towards adopting a model called Security Management Systems (SeMS), which aims to create a more pervasive security culture in air transportation.²¹⁵⁵ All participants, no matter what their specific role, would be responsible for maintaining security. Responsibility for security would not be limited to a particular department at the airport. Everyone would play a role in the security system, providing protection within their own area of responsibility, but also remaining vigilant about security breaches in other areas.²¹⁵⁶ The CATSA Advisory Panel stressed the importance of a security culture that engaged the entire airport community, one where all employees together worked as the “eyes and ears of aviation security.”²¹⁵⁷ The Panel suggested that members of the local community outside the airport should also be encouraged to participate.

The Panel stated that an effective airport security watch program would have several features:

- an integrated operational plan;
- proactive and methodical threat assessments;
- timely and appropriate communications;
- operational cooperation; and
- accountability that would extend to all layers.²¹⁵⁸

The Panel recommended rigorous security awareness programs for all airports.²¹⁵⁹ Such programs function much like “neighbourhood watch” programs. They would be guided by airport security committees, which would share relevant intelligence information with all front line staff. The Panel noted that some airports have already established security awareness programs. It praised the *iWatch* Airport Security Action Program at Halifax International Airport.²¹⁶⁰ The program encourages all individuals at the airport to be vigilant and to report potential security risks. The Halifax program has been adopted in other places, including Calgary and Vancouver.²¹⁶¹

²¹⁵⁴ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8112.

²¹⁵⁵ Testimony of Jim Marriott, vol. 37, May 31, 2007, pp. 4544-4545.

²¹⁵⁶ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8111-8112.

²¹⁵⁷ Exhibit P-169, p.48 of 202.

²¹⁵⁸ Exhibit P-169, p. 48 of 202.

²¹⁵⁹ Exhibit P-169, p. 48 of 202.

²¹⁶⁰ Testimony of Fred Jones, vol. 65, October 24, 2007, pp. 8111-8112.

²¹⁶¹ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8112.

Bertram testified that the security management program at Pearson International Airport was not limited to security awareness. He described a three-pronged approach which included engineering, enforcement and education (including security awareness). All employees who receive an RAIC must undergo a two-hour security awareness training program. This involves classroom instruction and testing, as well as specific training for those working in specialized areas, such as air traffic control and terminal operations. The goal is to develop a climate where security is not a department, but a way of thinking.²¹⁶²

Security awareness programs should continue to be encouraged. Such programs can help overcome complacency. The Commission notes, however, that the need for a robust security awareness program was identified by the 1985 airport security audit following the bombing of Air India Flight 182. A concept paper was developed then to enhance security awareness among airport workers and airport users.²¹⁶³ Also in 1985, the Seaborn Report identified a role for the travelling public in maintaining aviation security. Seaborn recommended that the public should be made aware of the security measures in place for its protection at airports and on board aircraft, and of the contribution the public can make to enhancing security.²¹⁶⁴

3.8.2.6 Conclusion

Airport security is a vital component of an effective civil aviation security regime. In 1985, shortly after the loss of Air India Flight 182, a review of security at Canada's airports revealed major deficiencies. These included inadequate control of access to restricted areas of airports and deficient perimeter security. In 2009, access control and perimeter security remain major vulnerabilities that require urgent attention. Poor control of airside portions of the airport leaves aircraft vulnerable to sabotage, a lesson that the history of air terrorism has taught many times.

Security threats can arise both outside the airport community and within it. Widespread organized crime involvement at Canada's airports, particularly those serving the largest cities, confirms that major lapses exist in airport security. Many failures of security that facilitate the presence of organized crime at airports can be exploited by terrorists.

Following the events of September 11, 2001, new security measures – NPS and the RAIC – were introduced to correct some shortcomings in access control. The RAIC provides a necessary additional layer to the aviation security matrix. However, the RAIC has yet to be fully implemented across Canada. NPS is also a key security measure, but the manner in which it has been implemented allows individuals to circumvent the screening process completely.

²¹⁶² Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8112-8113.

²¹⁶³ Exhibit P-101 CAF0695.

²¹⁶⁴ Exhibit P-101 CAF0039, p. 8 of 10.

The Commission urges full NPS at all Class 1 and Class 2 airports when individuals enter restricted areas, and random NPS at Class 1 airports when they leave. NPS should be extended to include searches of vehicles entering restricted areas at all Class 1 airports. Vehicle searches should occur at Class 2 airports when a risk assessment makes them advisable. CATSA is the appropriate screening authority to conduct all NPS operations and vehicle searches. CATSA should make it a priority to implement the RAIC at all 89 designated airports in Canada. It should also make it a priority to extend the RAIC system outside air terminal buildings to the airport perimeter, including vehicle gates, FBOs and tenant facilities.

As security measures to protect aircraft are strengthened, terrorists may well try to exploit remaining weaknesses in airport security. Public areas of air terminal buildings are susceptible to attack since they present targets of opportunity whenever large crowds gather there. Little protection currently exists for terminal buildings.

3.8.3 Fixed Base Operations and General Aviation

Fixed Base Operations (FBOs) and the General Aviation (GA) sector are largely unregulated. They represent a serious security vulnerability.²¹⁶⁵ FBOs operate charter and corporate flights,²¹⁶⁶ while the GA sector provides private aircraft for recreational flying, business aviation,²¹⁶⁷ charter services²¹⁶⁸ and specialty services, such as flight instruction and aerial work.²¹⁶⁹ Their facilities are often located at the periphery of designated airports²¹⁷⁰ and usually operate from separate terminals.²¹⁷¹

With scheduled commercial flights,²¹⁷² passengers and baggage must undergo multiple layers of screening.²¹⁷³ There is no such requirement for flights that depart the GA sector or FBOs. Passengers and baggage are allowed onto flights without any form of screening.²¹⁷⁴ Not surprisingly, most FBOs and GA establishments lack the capacity to screen²¹⁷⁵ and their premises are often poorly secured.²¹⁷⁶

²¹⁶⁵ Exhibit P-169, p. 55 of 202.

²¹⁶⁶ Exhibit P-169, p. 55 of 202.

²¹⁶⁷ Exhibit P-101 CAF0828, p. 7.

²¹⁶⁸ Final Submissions of the Attorney General of Canada, Vol. II, para. 416.

²¹⁶⁹ Exhibit P-101 CAF0828, p. 7.

²¹⁷⁰ In Canada, 89 airports have been designated to receive CATSA's screening services, and this represents approximately 99 per cent of all passenger traffic. Of the 89 designated airports, nine are considered Class 1, or major, airports, 20 are considered Class 2, or intermediate, airports, and 60 are considered Class Other, or smaller, airports. A non-designated airport does not have CATSA presence. See Exhibit P-169, pp. 103, 199 of 202; see also Exhibit P-172, p. 70 of 155.

²¹⁷¹ Exhibit 157, p. 120 of 135.

²¹⁷² "Scheduled" flights involve passengers who purchase the seats they occupy on the plane. Passengers on "non-scheduled" flights are non-paying passengers, such as are found on business and sports charters. See Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8150.

²¹⁷³ See Section 3.5.3, which describes the procedures and technology in place for screening passengers and baggage.

²¹⁷⁴ Final Submissions of the Attorney General of Canada, Vol. II, para. 402; see also Exhibit P-157, p. 120 of 135.

²¹⁷⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4632.

²¹⁷⁶ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8148.

Dr. Reg Whitaker, Chair of the CATSA Act Review Advisory Panel (CATSA Advisory Panel), testified that lack of screening at FBOs and GA establishments has often been justified on the grounds that the crew and passengers are generally “known entities.”²¹⁷⁷ For example, many of these facilities operate non-scheduled sports charters and business flights on which the crew members and passengers may fly repeatedly. Passengers have typically been authorized by, and are known to, their employers or team managers. They are believed to pose much less of a risk than an unknown individual who walks in “off the street”²¹⁷⁸ with a ticket for a scheduled commercial flight.²¹⁷⁹ Air Canada provides charter flights for national sports teams that fly from one unscreened FBO to another within Canada, and which do not normally connect to flights at other airports. Air Canada does not consider these charter services a major risk and, accordingly, does not see the need for many security measures.²¹⁸⁰

Some experts questioned this trust because of the history of threats to civil aviation.²¹⁸¹ Others agreed that many charter flights likely posed little risk, but nonetheless called for security procedures, although less extensive measures than “full-scale, multi-level screening.”²¹⁸² In no case did experts support the complete absence of security screening for passengers and baggage.

Many FBOs and GA facilities in fact provide other civil aviation services that present potentially high levels of recognized risk. Some facilities have begun to offer scheduled commercial flights²¹⁸³ that often rival the services provided by larger airlines operating out of main terminals. The rising popularity of such flights means that the number of passengers using FBOs and the GA sector is increasing. More passengers mean increased risk.²¹⁸⁴ Many large aircraft are used by FBOs and in GA operations, including wide-bodied jets that can carry large reserves of fuel,²¹⁸⁵ hundreds of passengers²¹⁸⁶ and significant volumes of cargo.²¹⁸⁷ There is a real concern that, in addition to targeting these facilities and aircraft for sabotage, terrorists could commandeer aircraft for use as suicide weapons or for dispersing chemical or biological weapons.²¹⁸⁸ With a comprehensive security regime lacking, FBOs and GA operations present significant opportunities for terrorism.

Both experts and stakeholders have noted the contradiction between the screening requirements at designated airports and those of FBOs and the

²¹⁷⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4632.

²¹⁷⁸ Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8150.

²¹⁷⁹ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8150, 8165; see also Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5265-5266.

²¹⁸⁰ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5266.

²¹⁸¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, pp. 5039-5040.

²¹⁸² Exhibit P-169, p. 55 of 202.

²¹⁸³ Final Submissions of the Attorney General of Canada, Vol. II, para. 402.

²¹⁸⁴ Exhibit P-169, p. 55 of 202.

²¹⁸⁵ Exhibit P-169, p. 55 of 202.

²¹⁸⁶ Exhibit P-157, p. 120 of 135.

²¹⁸⁷ Testimony Colin Kenny, vol. 38, June 1, 2007, p. 4695.

²¹⁸⁸ Exhibit P-169, p. 55 of 202; see also Testimony of Jacques Bourgault, vol. 38, June 1, 2007, p. 4633.

GA sector.²¹⁸⁹ Fred Jones, Vice President, Operations and Legal Affairs, for the Canadian Airports Council (CAC), stated that the CAC brought the issue to Transport Canada's attention, highlighting the inconsistent treatment of basically the same category of flight:

Our members raised concerns...about scheduled operations operating from the air terminal building that were subjected to the full spectrum of aviation and airport security while other scheduled operations of identical aircraft types were taking place from fixed-base operations in the absence of many elements of the existing security system which apply in and around the air terminal building....²¹⁹⁰

The security risks presented by FBOs and GA facilities, however, are not limited to unscreened passengers and baggage. Unscreened passengers from non-designated airports and FBOs may arrive at designated airports to proceed to scheduled flights. This commonly occurs in northern Canada. This has the potential to breach the security of "sterile" areas – areas of airports where the passengers and baggage have already been screened. Transport Canada explained that measures are in place to prevent screened and unscreened passengers from mixing in such circumstances,²¹⁹¹ but these measures are not always strictly followed, particularly at smaller airports. Unscreened FBO and GA passengers have mingled with screened passengers in sterile areas, including the airport tarmac, breaching the integrity of secure areas.²¹⁹² At one regional airport, two streams of passengers were separated merely by the use of an "invisible line."²¹⁹³ In its 2006 report, the CATSA Advisory Panel recommended that passengers and baggage transiting to scheduled flights be subject to full screening if not screened at their point of origin.²¹⁹⁴ The Commission agrees that this must become mandatory. It is a fundamental tenet of civil aviation security that unscreened passengers should never be permitted to mix with screened passengers.

Where FBOs and GA facilities are located on the grounds of designated airports, access to unauthorized or restricted areas is also a problem:

Any time you have a runway that has commercial aviation on one side and a fixed base operator or corporate aviation on the other side...you've got a whole different scheme of players now because they can all get across the flight line. They can taxi there. They can use their vehicles...there's a

²¹⁸⁹ See, for example, Exhibit P-169, p. 55 of 202.

²¹⁹⁰ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8148.

²¹⁹¹ Exhibit P-172, p. 69 of 155.

²¹⁹² Exhibit P-169, pp. 55-56 of 202.

²¹⁹³ Exhibit P-169, p. 56 of 202.

²¹⁹⁴ Exhibit P-169, p. 55 of 202.

manoeuvrability there that gives them access to areas on the secure side that we don't want them to have....²¹⁹⁵

Toronto's Pearson International Airport houses FBO and GA facilities within its restricted areas.²¹⁹⁶ The Greater Toronto Airports Authority (GTAA) considers that, since security controls govern access to restricted areas at Pearson, it is protected from threats that could originate from these poorly secured FBO and GA facilities. Vehicles entering restricted areas at Pearson must be escorted and only persons with the proper identification cards can be admitted.²¹⁹⁷ However, this confidence in these security controls may not be warranted. There are significant concerns about how effectively they are being applied. Indeed, access to restricted areas of airports is less than adequately controlled.²¹⁹⁸ Poor access control was highlighted recently at Pearson when the Minister of Transport and the Chair of the Standing Senate Committee on National Security and Defence (Senate Committee) themselves entered restricted areas improperly without being challenged.²¹⁹⁹

Recent reports by the RCMP,²²⁰⁰ Auditor General of Canada²²⁰¹ and Senate Committee²²⁰² about criminal activity at Class 1 airports demonstrate the porous nature of airside security at designated airports. Criminal organizations rely on persistent lapses in airport security to operate.²²⁰³ The lax security and presence of unscreened individuals at FBOs and GA establishments situated alongside restricted areas of airports magnify the risks of unlawful interference with civil aviation.

The security risks created by unauthorized access to restricted areas are heightened because, while FBO and GA establishments monitor their own access points to restricted areas, the regulatory tools for enforcing this monitoring are limited. The GTAA, which manages Toronto's Pearson International Airport, is ultimately responsible and accountable for access control for all airport tenants.²²⁰⁴ Tenants may hold lease agreements that are more than a decade old and that have not kept pace with changes in security requirements. There is no legal mechanism other than provisions in lease agreements for airport authorities to force tenants to comply with regulations, such as those that require monitoring of access points. Instead, airport authorities must rely on

²¹⁹⁵ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4984.

²¹⁹⁶ Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8164.

²¹⁹⁷ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8149-8150.

²¹⁹⁸ See Section 3.8.2, which discusses in detail the deficiencies in non-passenger screening and control of access to restricted areas of airports. See also Exhibit P-169, pp. 57-58 of 202; Exhibit P-172, p. 28 of 155.

²¹⁹⁹ Colin Freeze, "Operation Tarmac: politicians go undercover to expose security flaws at Pearson" *The Globe and Mail* (April 2, 2009), online: *The Globe and Mail* <<http://web.theglobeandmail.com/servlet/story/LAC.20090402.KENNY02/TPStory/National>>.

²²⁰⁰ Exhibit P-434, p. 2.

²²⁰¹ See March 2009 Status Report of the Auditor General of Canada, Chapter 1.

²²⁰² Exhibit P-172, p. 17 of 155.

²²⁰³ Exhibit P-172, p. 17 of 155.

²²⁰⁴ Testimony of Jim Bertram, vol. 65, October 24, 2007, p. 8163.

Transport Canada for enforcement.²²⁰⁵ The CAC called this a security weakness and articulated the need for greater “teeth” in the oversight mechanism of airport authorities, so that they can better enforce compliance with measures that fall within their mandate.²²⁰⁶

Finally, from a risk management perspective,²²⁰⁷ deciding that certain individuals pose minimal risk to civil aviation simply because they are “known,” without any formal screening by the civil aviation security community, is troubling. The Commission heard that passengers of many business and sports charter flights are considered trustworthy simply because they are recognized or established consumers familiar to the flight and security staff of the aviation companies with whom they regularly fly.²²⁰⁸

Even some individuals who have been vetted by the civil aviation security community, including through security background checks, have proved dangerous to civil aviation. The bombing of Pan Am Flight 103 in December 1988 was set in motion by the former head of security for Libyan Arab Airlines,²²⁰⁹ who used his knowledge to circumvent normal baggage check-in procedures at Malta’s Luqa Airport. According to Rodney Wallis, an international civil aviation security consultant, this “...portrayed the worst possible scenario facing legitimate governments with respect to attacks against civil aviation targets, namely direct involvement (rather than coercion) of airline staff with knowledge of and access to attack aircraft under cover of their legitimate roles.”²²¹⁰ There are other examples of civil aviation security incidents which involved “known” airport employees.²²¹¹ Chern Heed, a member of the CATSA Advisory Panel, described an analogous concept long employed for air cargo security in Canada, the “known shipper,”²²¹² as completely deficient as a security tool.²²¹³ Dr. Kathleen Sweet, an international civil aviation security expert, testified that the “...I know him, he’s OK” method of screening cannot be viewed as an appropriate security tool.²²¹⁴

The security vulnerabilities of FBOs and the GA sector appear to have been reported publicly for the first time in the Senate Committee’s January 2003 report, *The Myth of Security at Canada’s Airports*, although stakeholders had issued a call

²²⁰⁵ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8163-8164.

²²⁰⁶ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8161.

²²⁰⁷ See Section 3.3, which discusses risk management decision-making in civil aviation security.

²²⁰⁸ Testimony of Jim Bertram, vol. 65, October 24, 2007, pp. 8164-8165; see also Testimony of Yves Duguay, vol. 43, June 14, 2007, pp. 5265-5266.

²²⁰⁹ Wallis, *Lockerbie*, p. 59.

²²¹⁰ Wallis, *Lockerbie*, p. 38.

²²¹¹ In 1955, an aircraft cleaner was reportedly bribed to place an incendiary device in the wheel well of an aircraft; and in 1986, a customs officer with access to the flight line was charged with placing a bomb on board an Air Lanka aircraft. See Appendix A, Chronology: Significant Acts of Unlawful Interference with Civil Aviation.

²²¹² The concept involves accepting cargo for shipment on passenger aircraft, without the need of any security controls, where the shipper has an established business relationship with the airline and is therefore considered to be a “known shipper”; Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4630.

²²¹³ Testimony of Chern Heed, vol. 38, June 1, 2007, p. 4650.

²²¹⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4959-4960.

to action in 2002.²²¹⁵ The report stated that highly visible measures to strengthen aviation security in some areas left persistent gaps behind the scenes, including "...[a] lack of almost any kind of security requirements for private aircraft and their passengers."²²¹⁶ In 2007, the Senate Committee reported that little had changed, with FBOs and the GA sector still subject to "almost no scrutiny"²²¹⁷:

You can walk through those facilities without being identified. You can board charter aircraft without being searched, without ever producing your identification.... And while a manifest is given to the pilot of the plane, there is no checking of baggage, there's no checking that the individuals match the manifest, and so it seems to be an extraordinarily vulnerable place.²²¹⁸

Terrorists could easily exploit the widely reported²²¹⁹ gaps in FBO and GA security to gain access to aircraft and restricted areas of airports. For instance, a terrorist could simply pose as a passenger at one of these facilities.

Transport Canada acknowledged the deficiencies in FBO and GA sector security and consulted with stakeholders. It developed a proposal that at least some stakeholders believe is a legitimate attempt to balance the concerns of the operators of these facilities with the need to resolve the security threats they face.²²²⁰ Currently, however, these facilities remain inadequately protected and their passengers and baggage remain unscreened.

Wallis testified that, particularly where FBOs and GA facilities feed into major transit points, passengers and baggage must be subject to screening.²²²¹ With passengers and baggage a stated priority of the federal government's strategy in aviation security,²²²² it is surprising that the security issues facing this sector have not been wholly addressed. As well, in the post-September 11th world, the risk of an aircraft being overtaken and used as a weapon is known.²²²³ A multi-layered, risk-based approach to security demands adequate protection for all domains of risk.²²²⁴ Although full-scale security akin to that at Class 1 airports may not be necessary for all FBO and GA establishments, the current lack of security must not continue.

²²¹⁵ Exhibit P-101 CAF0847, p. 6 of 17.

²²¹⁶ Exhibit P-171, p. 14 of 256.

²²¹⁷ Exhibit P-172, p. 69 of 155.

²²¹⁸ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4696.

²²¹⁹ Exhibit P-172, p. 69 of 155; see also Exhibit P-169, p. 51; see also Exhibit P-171, p. 14 of 256.

²²²⁰ Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8149.

²²²¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5039.

²²²² Exhibit P-411, p. 9; see also Exhibit P-101 CAF0872, p. 2.

²²²³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4632.

²²²⁴ Exhibit P-361, Tab 1, p. 9; see also Section 3.3, which discusses risk management decision-making in civil aviation security.

3.8.3.1 Enhancing Security and Meeting the Needs of Industry

In 2006, the CATSA Advisory Panel recommended that FBOs and the GA sector receive closer attention and regulation. The Panel noted that many small GA operations pose little security risk and that stricter government regulation could be disproportionately onerous and costly. Like the experts, stakeholders noted that security which is too intrusive or expensive could harm the industry.²²²⁵ Captain Craig Hall, Director of the National Security Committee of the Air Line Pilots Association, International (ALPA), which advocates screening passengers and baggage at FBOs and GA facilities, stated:

...[W]e have to always keep in mind that we can't take measures that are so punitive that they destroy our industry, but at the same time we have to balance that by making sure that we are able to take the measures that need to be taken.²²²⁶

Hall testified that security concerns must not be minimized.²²²⁷ Similarly, Whitaker stated that a balance between security and industry needs is required.²²²⁸

In 2006, the CATSA Advisory Panel recommended extending passenger screening to FBOs where the size of the operation warrants such screening.²²²⁹ Sweet testified about care that must be taken to ensure that all facets of risk in a given situation are evaluated, not just the size of the airport. For example, a small airport in a remote location may still carry great risk if it is situated close to critical infrastructure, such as a nuclear power plant or chemical manufacturing plant.²²³⁰ In 2007, the Senate Committee recommended that all persons and vehicles, including private aircraft, be searched at all FBOs attached to Canada's 89 designated airports.²²³¹ Stakeholders have generally agreed that any decision to require screening of commercial passengers on aircraft departing from facilities that are located away from air terminal buildings, which is currently being considered by Transport Canada, must be based on threat, vulnerability and risk assessments, as well as cost-benefit analyses.²²³²

Transport Canada reported that many operators of FBO and other facilities have taken steps, even without security requirements, to improve physical security and to mitigate risk through increased security awareness.²²³³ The GA community has implemented security awareness initiatives to encourage a "neighbourhood watch" approach to security. Such practices have included managing the keys to aircraft and facilities, ensuring that equipment is locked or secured, and noting and challenging suspicious activity. Sweet recommended that every FBO and

²²²⁵ Exhibit P-101 CAF0847, p. 7.

²²²⁶ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8017.

²²²⁷ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8016.

²²²⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 5484.

²²²⁹ Exhibit P-169, p. 56 of 202.

²²³⁰ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4985.

²²³¹ Exhibit P-172, p. 71 of 155.

²²³² Exhibit P-101 CAF0847, p. 7.

²²³³ Exhibit P-101 CAF0847, p. 8.

GA facility draft and implement a security plan²²³⁴ and be well-informed about airport functioning from a security perspective.²²³⁵

A culture of security awareness, a desirable and necessary foundation for improved security, may be sufficient for some smaller establishments where the security risk is low. However, security awareness alone is not sufficient for FBOs and the GA sector in general.

Logistical issues arise about the physical location of screening and the authority to be responsible for it.²²³⁶ The CATSA Advisory Panel and the Senate Committee both saw CATSA as the appropriate agency to oversee screening if it is extended to FBOs and the GA sector.²²³⁷ CATSA's current screening mandate does not include flights from FBOs or from the GA sector.²²³⁸

Some stakeholders worried that, without additional resources, CATSA might become overburdened by screening FBOs and might not be able to accommodate the 24-hour operation of some FBOs. They suggested that CATSA consider training existing security personnel at facilities such as FBOs to perform authorized searches as agents of CATSA. CATSA stated that additional funds would be necessary for training FBO personnel to perform such searches and that any such arrangement would require further analysis.²²³⁹

The CATSA Advisory Panel concluded that "...too many risks and too many questions" surround the GA and FBO sectors to leave their security deficiencies unaddressed.²²⁴⁰ The Commission agrees.

3.8.3.2. Transport Canada: Action Taken but More Required

Transport Canada has recognized the security risks presented by the lack of screening at FBOs and GA operations. However, it has acted slowly in response. In the meantime, FBOs and the GA sector remain relatively unprotected and vulnerable to attack.²²⁴¹

In late 2002, Canada's aviation stakeholders recommended that Transport Canada review FBO and GA security.²²⁴² In the spring of 2004, Transport Canada launched a review of unscreened commercial flights, aiming to achieve more consistent security across all commercial operations. As part of this review, the Department held extensive consultations with stakeholders,²²⁴³ conducted a

²²³⁴ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4985.

²²³⁵ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, p. 4986.

²²³⁶ Exhibit P-169, p. 56 of 202.

²²³⁷ Exhibit P-169, p. 56 of 202; see also Exhibit P-172, p. 69 of 155.

²²³⁸ Exhibit P-101 CAF0847, p. 4.

²²³⁹ Exhibit P-101 CAF0847, p. 8 of 17.

²²⁴⁰ Exhibit P-169, p. 56 of 202.

²²⁴¹ Exhibit P-169, p. 55 of 202.

²²⁴² Exhibit P-101 CAF0847, p. 6 of 17.

²²⁴³ Exhibit P-101 CAF0847, pp. 1-2 of 17.

risk assessment²²⁴⁴ and reviewed how other countries tackled the problem.²²⁴⁵ It also examined the effects of potential changes on industry operations, as well as the delivery of screening services and funding.²²⁴⁶

In September 2005, draft recommendations²²⁴⁷ were distributed to stakeholders, and further consultations were held in the spring of 2006.²²⁴⁸ Many stakeholders endorsed the recommendations or were neutral, but some were concerned about the significant financial and operational impacts, especially for private charter operations.²²⁴⁹ Many suggested that individual charter operations be allowed to customize their manner of compliance to take account of the sometimes unique characteristics of their operations.²²⁵⁰

In July 2006, Transport Canada reported that it anticipated phasing in screening requirements for FBOs beginning in early 2007. The Attorney General of Canada reported, however, that the effort was hampered by CATSA's claim that it needed additional funding.²²⁵¹

Security improvements in the GA sector suffered a similar fate. In 2002 and 2003, Transport Canada advisories were issued to the GA community to provide guidance for security measures.²²⁵² However, a GA "Task Team" was not created until 2007 to review security issues regarding general aviation in Canada. In May 2008, Transport Canada reported that the GA Task Team had "...met several times to date, and further discussions will be scheduled as required to advance the work in this area."²²⁵³

In 2006, the CATSA Advisory Panel criticized the delay in addressing gaps in FBO and GA security, although it acknowledged the complexities in designing and implementing a security regime in this area.²²⁵⁴ The following year, the Senate Committee also criticized the delay:

²²⁴⁴ Final Submissions of the Attorney General of Canada, Vol. II, para. 408. Transport Canada's current risk assessment and risk management procedures have been questioned. The Commission was not provided with a copy of any risk assessment conducted on the issue of FBOs or the GA sector. See, generally, Section 3.3, which examines risk management procedures in civil aviation security and the process used by Transport Canada.

²²⁴⁵ Transport Canada noted that the international community has also recognized the vulnerability of FBOs and the GA sector and has taken steps to improve security at such facilities. G8 countries, in particular, have expressed a commitment to developing international standards for enhancing FBO and GA security. In Europe, some airports conduct screening at FBOs, where it is largely the responsibility of airport operators. In the United States, there has been a strong separation between FBOs and mainstream commercial traffic. See Exhibit P-101 CAF0847, p. 6; see also Exhibit P-101 CAF0827, p. 6.

²²⁴⁶ Final Submissions of the Attorney General of Canada, Vol. II, para. 408.

²²⁴⁷ The recommendations are considered sensitive security information and cannot be publicly disclosed.

²²⁴⁸ Exhibit P-101 CAF0847, p. 11.

²²⁴⁹ Exhibit P-101 CAF0851, p. 13.

²²⁵⁰ Exhibit P-101 CAF0847, p. 12.

²²⁵¹ Final Submissions of the Attorney General of Canada, Vol. II, paras. 412, 413.

²²⁵² Final Submissions of the Attorney General of Canada, Vol. II, para. 417.

²²⁵³ Exhibit P-101 CAF0827, p. 9 of 19.

²²⁵⁴ Exhibit P-157, p. 120 of 135.

The time for considering should be long past. Fixed-Base Operations on the periphery of airport terminals present the same potential threats as passenger and cargo terminal operations. Fairly large aircraft leave from some of these operations. With no screening, what is to prevent a terrorist from commandeering one of these planes and flying it into a building?²²⁵⁵

3.8.3.3 Conclusion

FBOs and the GA sector are subject to few security requirements. These operations sometimes use large aircraft and transport large numbers of passengers. Yet FBO and GA facilities are not required to screen passengers or their baggage, nor are security measures generally imposed on their premises. Terrorists will naturally seek areas of weakness. Relatively unprotected FBOs and GA facilities provide prime targets. The largely unhindered access to aircraft makes their use as weapons a major security risk.

FBOs and GA facilities were identified as uniquely vulnerable to terrorist attack as early as 2002. However, security measures still have not been implemented. With the GA sector, enhanced security is still at the discussion stage. As the Senate Committee noted, the time for discussion is over. At a minimum, passengers and baggage must be screened at FBO and GA facilities that feed into designated airports or are located on airport premises. The facilities themselves must also be secured, guided by a written security plan. Training is necessary to foster a culture of security awareness.

CATSA is the appropriate screening authority, given that it already fills this role at main terminal buildings. The Government must change regulations and provide adequate funding for security measures. Measures should be implemented based on risk, taking into account that different FBO and GA establishments may face different risks. These measures will fill a serious security gap and contribute to the multi-layered approach necessary for an effective security regime in civil aviation as a whole.

3.9 Duty to Warn and Transparency in Aviation Security

Although the Government of Canada was aware of numerous threats against Air India in the year leading up to the Air India bombing,²²⁵⁶ it did not notify the public about them. By June 1985, the Government was also aware of deficiencies in the airline's security measures. Transport Canada's position before the Commission was that it had neither the jurisdiction nor the duty to ensure the appropriate implementation of screening measures by Air India at the time of the bombings. Dale Mattson, Transport Canada's Manager of Safety

²²⁵⁵ Exhibit P-172, p. 71 of 155.

²²⁵⁶ See Volume Two: Part 1, Pre-Bombing, Section 1.12, A "Crescendo" of Threats.

and Security at Pearson International Airport in 1985, also stated that there was no regulatory duty to warn the public about threats against airlines or about deficiencies in air carrier procedures.²²⁵⁷ The Government had effectively decided to leave essential aspects of security implementation and decision-making with third party private enterprises: airlines and their security companies.

Even if the Government were, as it claimed, powerless to effect an appropriate security response in 1985, it can be argued that it had a duty to warn the travelling public about at least some security and threat information about Air India. Passengers could then make informed travel decisions. During Phase I of the Commission's work, victims' family members raised precisely this issue, asking whether in 1985 there should have been, and whether there currently needs to be, a public warning system about the threats facing an airline.²²⁵⁸ During the work of the Commission, the need for greater transparency in civil aviation security was repeatedly raised, as were countervailing concerns about safeguarding national security, preserving the air travel industry and preventing undue alarm.

Because of poor communication about threats in 1985, some civil aviation stakeholders were not aware of the heightened threat facing Air India. Such information could have led to a dramatically different outcome, one with no lives lost. In particular, air carriers interlining passengers and baggage to Air India were not made aware of the threat to Air India, even though this information would probably have caused them to alter their security operations. Had Canadian Pacific (CP) Air been warned, it is almost certain that more vigilance would have been exercised in the decision to interline the "M. Singh" bag to Air India Flight 182 in the absence of a reservation for M. Singh, despite a business culture that stressed customer satisfaction.²²⁵⁹ The *Canadian Air Transport Security Authority Act Review Advisory Panel* (CATSA Advisory Panel)²²⁶⁰ concluded that threat information was inadequately shared in 1985:

This somewhat tangled tale highlights a crucial weakness in the chain of intelligence communication. Even where intelligence was available in advance that gave warning of the kind of threat that tragically materialized on June 23, 1985, the linkage to those bodies with capacity to take appropriate security measures remained problematic. Nowhere is the problem of inadequate threat communication more apparent than in the manner in which two bags containing bombs were allowed to be loaded on two CP Air flights, and interlined to

²²⁵⁷ Testimony of Dale Mattson, vol. 29, May 16, 2007, pp. 3258-3259.

²²⁵⁸ See, for example, Testimony of Perviz Madon, vol. 6, October 4, 2006, p. 601.

²²⁵⁹ Exhibit P-157, pp. 64-65 of 135.

²²⁶⁰ The Panel was appointed to conduct a five-year review of the CATSA Act. The Minister of Transport also directed the Panel to "review the actions taken since 1985 to address the specific aviation security breaches associated with the Air India flight 182 bombing, particularly those relating to the screening of passengers and their baggage" and "to advise the Minister on whether further changes are required in legislation, regulations or practice to specifically address these breaches": Exhibit P-157, p. 11 of 135.

a high-risk carrier. The story of the Canadian Pacific check-in official in Vancouver who was harassed by passenger ‘M. Singh’ into permitting the fatal bag to be interlined to Air India Flight 182 ... is now well known. If all air carriers in Canada with flights connecting to Air India had been warned that Air India was under special security alert, the CP Air agent might have exercised more caution. If, as would happen today, Transport Canada had given direction to all airlines not to interline any baggage to Air India flights, the two individuals in question might have been deterred at the CP Air check-in. It seems, however, that the practice in place in 1985 did not include communication of threat warnings to other connecting airports and airlines.²²⁶¹

An emphasis in 1985 on secrecy and the “need-to-know” principle hindered the communication of important information to some who required it – in particular, front-line staff making key, on-the-spot decisions. As the CATSA Advisory Panel stated, “[t]he Air India tragedy illustrates what happens when excessive concern with secrecy gets in the way of sound operational decisions.”²²⁶²

Many have now called urgently for a move to a new “need-to-share” principle for security intelligence, while at the same time they recognize the imperative to maintain secrecy where necessary, and to honour any attached caveats.²²⁶³ Clearly, the public must be considered a stakeholder in civil aviation security. The question of how much information relating to security risks and deficiencies in security measures can and should be shared with the public will depend on the nature of the threat, the potential risks associated with disclosure and the need to prevent disruption within the aviation industry on which the public relies.

3.9.1 Public Warning System for Security Threats against Airlines

Members of the victims’ families stated that had information about threats to Air India been made public in 1985, at least some victims would have chosen not to fly on Air India.²²⁶⁴ Over the course of the Commission’s hearings, several aviation security experts and stakeholder representatives were asked about the need for a public warning system about threats to airlines. They largely rejected such a system as being neither desirable nor feasible.

Even the idea of a general notification system to inform the public about ambient threat levels against the country at large was dismissed as impractical.²²⁶⁵ Dr. Reg Whitaker, Chair of the CATSA Advisory Panel, described the colour-coded public notification system implemented by the Department of Homeland Security

²²⁶¹ Exhibit P-157, p. 50 of 135.

²²⁶² Exhibit P-157, p. 50 of 135.

²²⁶³ Exhibit P-169, p. 43 of 202.

²²⁶⁴ See, for example, Testimony of Perviz Madon, vol. 6, October 4, 2006, p. 601.

²²⁶⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

(DHS) in the US²²⁶⁶ after the 2001 terrorist attacks as both a failure and an object of some derision.²²⁶⁷ He testified that, after a certain point, the public generally stopped paying attention to the stated threat levels and the system would lose its effectiveness.²²⁶⁸ When asked whether a similar notification system ought to be adopted in Canada, Whitaker responded, “[a]bsolutely not.”²²⁶⁹

Rodney Wallis, an expert in international civil aviation security and former International Air Transport Association (IATA) Director of Security, examined the issue of publishing warnings about threats against airlines in his 1993 book, *Combating Air Terrorism*. Before the bombing of Pan American (Pan Am) Flight 103 in December 1988,²²⁷⁰ he wrote, there had been limited public disclosure about a specific threat against Pan Am:²²⁷¹

Much has been written and broadcast on the subject of the Helsinki warning. The information had been circulated to other U.S. embassies and at least one (in Moscow) had posted the details on a notice board, thus enabling those with access to it and intending to fly to the United States to reassess their traveling plans should they wish to do so. The information was generally made available throughout the two-thousand-strong U.S. community in the Russian capital city. It was not freely circulated in other countries. It is a point the families and friends of the victims have reverted to again and again, although the inquiry conducted by a specially constituted presidential commission did not find any individuals who changed their plans as a result of the threat being made known to them. Even so, to tell or not to tell has become an international debate.²²⁷²

²²⁶⁶ The US Department of Homeland Security’s Color-coded Threat Level System “is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack.” Raising the threat condition has economic, physical, and psychological effects on the nation; to mitigate this, the Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information: US Department of Homeland Security, *Homeland Security Advisory System*, online: US Department of Homeland Security <http://www.dhs.gov/xinfo/share/programs/Copy_of_press_release_0046.shtm> (accessed November 3, 2009).

²²⁶⁷ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁶⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁶⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁷⁰ The bombing of Pan Am Flight 103 is generally considered a “copycat” terrorism incident because it replicated the precise method of sabotage used to destroy Air India Flight 182. See Wallis, *Combating Air Terrorism*, p. 26.

²²⁷¹ A threat against Pan Am had been made on December 5, 1988, through a telephone call received by the United States Embassy in Helsinki warning that a bombing attack would take place “within the next two weeks” against a Pan Am aircraft operating between Frankfurt and the United States. It gave details of the persons who would allegedly carry out the crime and of the proposed methodology. Experts agreed this was a detailed threat to be taken very seriously, but Finnish and US government authorities later decided that the warning was a hoax. Pan Am Flight 103 was destroyed by a bomb on December 21, 1988, killing 270 people. See Wallis, *Combating Air Terrorism*, pp. 26–28.

²²⁷² Wallis, *Combating Air Terrorism*, p. 28.

Wallis concluded that public warning systems miss their mark because, paradoxically, they can promote terrorism. The rationale for publicizing threats to airlines is to provide information to the public, and people may choose not to travel as a result. Counting on this very response, terrorists could use the threats themselves as weapons to obliterate an airline's customer base. This would not only have repercussions for the viability of the airline, but potentially for the entire air travel industry. The prospect of encouraging hoax threats and "copycat" behaviour further diminished the possible value of such warning systems. In the end, both the aviation industry and the public would be victimized:

The general rule must be *not* to advertise threats against airlines. First, to do so would hand a new weapon to the terrorists. These criminals would need only to phone in a threat to drive an airline's customers away, assuming the intending passengers reacted in the manner suggested by the protagonists of the "tell" policy. Used as a weapon, this method could decimate a nation's air services with no danger to the perpetrators. Second, widespread advertising of bomb threats would encourage a multiplication of the hundreds upon hundreds of hoax bomb calls made to airlines every year. As fire and ambulance emergency services know only too well, there are many maladjusted people who get some sort of perverted thrill from such behavior. The airlines suffer from these same individuals. The "copycat" syndrome would come well to the fore if threats were to become published. The final victims are, of course, the passengers.²²⁷³

Whitaker also rejected as "impractical"²²⁷⁴ a public warning system for security threats against airlines. He contended that warnings to the public were not necessary if a specific threat was directed against a flight, since there were already adequate security responses in Canada. The flight would be grounded or other appropriate measures taken.²²⁷⁵ Wallis agreed, noting that, where additional security measures were instituted, passengers would become aware of the problem and would need assurance that sufficient procedures were in place to protect them.²²⁷⁶ Passengers might change their itineraries, but this would occur "...without the publicity that general broadcasting would bring and with minimum satisfaction going to the perpetrators."²²⁷⁷ Whitaker described a public warning system for non-specific threats as impractical, citing commercial grounds as the primary concern:

²²⁷³ Wallis, *Combating Air Terrorism*, pp. 28-29 [Emphasis in original].

²²⁷⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁷⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁷⁶ Wallis also noted that, at least at the time, bomb threats against airlines were extremely common. A study of bomb threats undertaken by airlines in the United States during a ten-year period between the late 1970s and early 1980s demonstrated that "no warning had ever led to the discovery of a bomb. More than ten thousand cases were investigated": Wallis, *Combating Air Terrorism*, pp. 29-30.

²²⁷⁷ Wallis, *Combating Air Terrorism*, p. 30.

...[I]f there is a specific threat, then the flight doesn't take off. If there is not a specific threat, you can't issue warnings and consumer advisories that would have enormous implications for the...commercial viability of whole airlines...on the basis of speculative intelligence.²²⁷⁸

Although security was always the primary objective, Transport Canada officials advised that a "triangle" of factors often had to be considered when implementing security measures. These included effective security, the efficiency of the aviation industry and respect for individual rights.²²⁷⁹ Whitaker testified that a public warning system did not strike the right balance between security and industry concerns.

Counsel for the Air India Victims' Families Association acknowledged that public warnings for purely speculative threats provided little value. However, counsel questioned favouring a blanket protection for the commercial interests of airlines over the security of the travelling public. Counsel argued that something less than a specific threat might sometimes warrant a public warning by government, and that some individuals could then choose not to fly with a particular air carrier. For example, a threat might be acknowledged by the appropriate national security agencies as well as by the airline, but not be directed at a specific flight.²²⁸⁰ As well, the general public might not be aware of the heightened threat under which some airlines regularly operate. The question was raised before the Commission whether, when threats are specific enough to justify assigning extra security, the public, as well as ticket and travel agents, should be notified.

Some experts opposed a full-scale public notification system managed by government, but gave some support to promoting at least a limited awareness of threats once a certain threshold was reached.²²⁸¹ Whitaker testified that ticket agents should be notified in such a situation, just as CP Air and other air carriers interlining passengers to Air India in 1985 should have been notified of the heightened threat then facing Air India.²²⁸² The CATSA Advisory Panel stated that Transport Canada would provide direction to air carriers today.²²⁸³ Whitaker argued that providing public warnings was not objectionable in principle,²²⁸⁴ but that that such a system would be unworkable in practice. He questioned the

²²⁷⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁷⁹ Testimony of Jean Barrette, vol. 38, June 1, 2007, p. 4567.

²²⁸⁰ Norm Boxall, Counsel for the Air India Victims' Families Association, posed the following question: "...I could understand why if it's a purely speculative matter why the public wouldn't be warned. But if we're dealing with a situation where the RCMP acknowledged the threat; CSIS acknowledged the threat; the airline itself acknowledged the threat and says it's a threat...why should the public not know? Why do we have to protect the commercial interest of that airline? Why shouldn't the customer know the threat?": Transcripts, vol. 38, June 1, 2007, p. 4612.

²²⁸¹ Testimony of Michael Hennessey, vol. 14, November 8, 2006, p. 1357; Testimony of William Leiss, vol. 91, December 7, 2007, p. 12015.

²²⁸² Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4613.

²²⁸³ Exhibit P-157, p. 50 of 135.

²²⁸⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4607-4608.

appropriateness, in the absence of specific intelligence, of government-issued advisories about particular airlines when these could harm their competitiveness and viability.²²⁸⁵ He made no comment about the advisability of informing travel agents about non-specific threats to airlines.²²⁸⁶

A counsel for the families noted a potential inconsistency, however, since the Government of Canada had what seemed to him an analogous public warning system – foreign travel advisories. Advisories warned about situations abroad that might affect the safety and security of the travelling public,²²⁸⁷ including the threat history of certain countries and expected future threats. The advisories were intended to enable the public to make informed decisions to minimize risks while abroad.

Whitaker testified that warnings issued about an entire country were qualitatively different from those about a specific airline operating as a private enterprise in Canada. He agreed that travel advisories about some foreign destinations may have the unintended effect of discouraging travel on particular airlines,²²⁸⁸ but cautioned that there were “considerable implications” for a government that issued a “consumer advisory” identifying a particular airline as riskier than others.²²⁸⁹

Wallis agreed that, while one would expect governments to issue travel advisories about countries with security problems, the concept of governments advising the public about individual airlines under threat would be “...getting into some difficult areas.”²²⁹⁰ He stated that the circumstances would have to be “pretty powerful” for a government to issue any warning about a specific airline, and that, to date, he had not seen a situation to justify such a warning.²²⁹¹ In his 1993 book, he stated that such warnings could effectively shut down the operation of an airline.²²⁹²

Dr. William Leiss, an expert in risk management, differed about the proper role of government. He testified that the duty to warn the public is a significant issue in the field of risk management. Since Transport Canada held the ultimate authority over Canadian airspace, the Department arguably had a duty to make critical threat information public, particularly where an airline was not responding appropriately to threats. Nevertheless, he agreed broadly with Wallis that only particular circumstances would trigger the need for government to issue a warning.²²⁹³

²²⁸⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4593.

²²⁸⁶ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4613.

²²⁸⁷ Anand questioning of Reg Whitaker, Transcripts, vol. 38, June 1, 2007, pp. 4605-4606. See also Foreign Affairs and International Trade Canada, “Travel Reports & Warnings,” online: Foreign Affairs and International Trade Canada <http://www.voyage.gc.ca/countries_pays/menu-eng.asp> (accessed November 3, 2009).

²²⁸⁸ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4606.

²²⁸⁹ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4606.

²²⁹⁰ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5062.

²²⁹¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5063.

²²⁹² Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5063.

²²⁹³ Testimony of William Leiss, vol. 91, December 7, 2007, p. 12015.

In its Final Submissions, the Attorney General of Canada expressed concern that the Commission did not hear sufficient evidence about whether government officials had a legal or ethical duty to warn the public. The Attorney General submitted that a more thorough investigation was warranted to address:

- whether, and under what circumstances, the public was warned of threats to airlines in Canada, if ever;
- whether other countries impose a duty to warn on their governments; and
- the policy and legal implications of warning the public, including liability to air carriers whose operations could be compromised by speculative or classified intelligence.²²⁹⁴

Experts before the Commission gave considerable weight to commercial considerations, opposing a general public notification system for threats to airlines. Some agreed that a public warning might be warranted on reaching a certain threat threshold, but there was difficulty in articulating the threshold. The consensus seemed to be that it would be difficult to achieve the correct balance between security and efficiency, at least as the proposal for a warning system was currently understood. In short, a public warning system did not find widespread support among aviation security experts.

3.9.2 Informing the Public: Greater Transparency Required in Civil Aviation Security

It was acknowledged, however, that greater transparency, as opposed to publicity, about measures taken to enhance aviation security could increase public confidence in aviation security.²²⁹⁵

Still, secrecy is important to prevent terrorists from learning about specific security measures.²²⁹⁶ The *Aeronautics Act*²²⁹⁷ enforces secrecy by prohibiting the disclosure of the details of security measures:

4.79 (1) Unless the Minister states ... that this subsection does not apply in respect of a security measure, no person other than the person who made the security measure shall disclose its substance to any other person unless the disclosure is required by law or is necessary to give effect to the security measure.

However, accountability in aviation security is also important. The Commission heard from many experts and stakeholders who were concerned about

²²⁹⁴ Final Submissions of the Attorney General of Canada, Vol. II, paras. 258, 261.

²²⁹⁵ Testimony of Reg Whitaker, vol. 38, June 1, 2007, pp. 4602-4603.

²²⁹⁶ See Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4603.

²²⁹⁷ R.S.C. 1985, c. A-2.

unnecessary secrecy in aviation security.²²⁹⁸ The Commission was dismayed to learn that the Government had long known about many significant gaps in civil aviation security – particularly those relating to air cargo,²²⁹⁹ airside security,²³⁰⁰ Fixed Base Operations (FBOs) and the General Aviation (GA) sector²³⁰¹ – but had failed, in some cases for decades, to address these deficiencies. The need for secrecy must not shield government and prevent reasonable disclosure of aspects of the aviation security program to the public. The public deserves assurances that security measures actually enhance security and that the resources expended are both justified and wisely allocated. Greater public awareness of the sufficiency of security measures can also deter terrorism.²³⁰²

The Commission recognizes the need to balance secrecy with public confidence. On one hand, this requires disclosing information to reassure the public that the security system is sufficiently rigorous; on the other, it requires safeguarding information which, if it falls into the wrong hands, could harm aviation. Aviation security experts suggested various ways to achieve this balance, but generally agreed that greater transparency is required about many aspects of aviation security. Among the policies and measures requiring greater public disclosure were:

- Risk management methodologies and the risk rationale for resource allocation;
- The rationale for establishing the Passenger Protect Program, the selection criteria used for the Specified Persons List (SPL) and the process for removal of a name from the list;
- Uses of “invasive” technology; and
- The collection and expenditure of user fees, such as the Air Travellers Security Charge (ATSC).

On risk management, the Commission heard that the Government and stakeholders should provide the public with sufficient information, without compromising national security, about the methodology used to assess and manage aviation security risks, to justify the way resources are allocated. Such information could strengthen confidence in the public institutions responsible for civil aviation security.²³⁰³ As Leiss testified:

I think we have enough evidence – certainly that I’ve seen before the Commission – to suggest that we need a higher level of accountability which [would enable] us to have a higher level of confidence that the requirements of a risk

²²⁹⁸ See, for example, Exhibit P-172, pp. 78-82 of 155.

²²⁹⁹ See Section 3.8.1, which discusses deficiencies in air cargo security.

²³⁰⁰ See Section 3.8.2, which discusses deficiencies in airport security.

²³⁰¹ See Section 3.8.3, which discusses deficiencies in FBO and GA security.

²³⁰² See, for example, Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5282. See also Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8072.

²³⁰³ Testimony of William Leiss, vol. 91, December 7, 2007, pp. 11960-11961.

management [and] a risk-based decision-making approach, are being fulfilled by all parties, all together....²³⁰⁴

The Privacy Commissioner of Canada, Jennifer Stoddart, testified that, where security measures are intrusive and could violate individual rights, more extensive disclosure would be required.²³⁰⁵ For example, the Passenger Protect Program drew criticism from experts about the lack of disclosure about the rationale for the Program,²³⁰⁶ the vague criteria used to select individuals for the SPL²³⁰⁷ and the sparse details about the reconsideration process.²³⁰⁸ Stoddart also raised the concern that invasive measures could be employed for purposes other than security, such as the use of radio-frequency identification (RFID) technology on boarding passes by airport retailers to track passenger movements within the terminal. She stated that, where security measures are used to serve non-security objectives, passengers need to be properly informed to ensure that they are free participants and that they fully consent.²³⁰⁹

Stakeholders strongly opposed in principle the use of passenger fees to fund aviation security and insisted on proper accounting to track the collection and use of such fees if the Government nonetheless introduced them. Stakeholders wanted assurance that the funds were invested solely in aviation security and that they were not used to subsidize other modes of transportation, such as marine or rail.²³¹⁰ The ATSC, a fee collected from passengers expressly to fund aviation security, was widely condemned because of the lack of comprehensive accounting applied to its collection and disbursement, and for the inability to trace the ultimate investment of these funds.²³¹¹

The question of whether the results of intrusion tests should be made public also sparked controversy. These are tests by Transport Canada of the security screening system. Prohibited items, such as guns, knives and explosives, or replicas, are surreptitiously passed through security checkpoints to determine whether the screening process detects them. The Standing Senate Committee on National Security and Defence (Senate Committee), which generally called for greater public awareness of the shortcomings in civil aviation security,²³¹² observed that test results were regularly made public before September 11, 2001, but that they were not publicly available after.²³¹³ The Committee stated that high-level sources in government had reported that the failure rate of these intrusion tests – the percentage of prohibited items that get through screening undetected – was “in the double digits.” Noting that, “...if the public knew the

²³⁰⁴ Testimony of William Leiss, vol. 91, December 7, 2007, p. 12010.

²³⁰⁵ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, pp. 9072-9073.

²³⁰⁶ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, pp. 9016-9017.

²³⁰⁷ Testimony of David Lyon, vol. 40, June 5, 2007, p. 4870.

²³⁰⁸ Exhibit P-278, Tab 6, p. 14.

²³⁰⁹ Testimony of Jennifer Stoddart, vol. 72, November 6, 2007, pp. 9067-9068.

²³¹⁰ See, for example, Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8139.

²³¹¹ Exhibit P-169, pp. 168-170 of 202.

²³¹² Exhibit P-172, p. 80 of 155.

²³¹³ Exhibit P-172, p. 81 of 155.

real figures people would be clamoring for action,"²³¹⁴ the Senate Committee was a strong proponent of publicizing intrusion test results:

...[W]e are very concerned that Canadians are not being made aware of [test results] for two reasons. One, we believe Canadians have a right to choose, with as much knowledge as reasonable, what risks they want to undertake. And secondly, there's a great deal of money going into the process of screening people and Canadians have a right to know whether or not it is an effective process, so we believe that these results should be made public.²³¹⁵

Both Wallis and Yves Duguay, Senior Director of Security at Air Canada and Chairman of the IATA Security Committee, disagreed with releasing the results of intrusion tests.²³¹⁶ They felt that disclosure would alarm the public unnecessarily while possibly identifying weaknesses in security measures to those who might want to cause harm. The Government of Canada cited the possibility of identifying weaknesses to justify keeping the results of these tests from the public.²³¹⁷

The Senate Committee argued that this concern could be alleviated by delaying the release of test results by six to ten months, or some other reasonable period, to allow flaws identified in the system to be corrected.²³¹⁸ Wallis said he could accept release of such information only if both conditions – correction of failures, and elapse of time since testing – had been met.²³¹⁹ Senator Colin Kenny, Chair of the Senate Committee, told the Commission that the value of public disclosure lay in informing the public and in providing the necessary incentive for the Government to address the deficiencies in a timely and effective manner:

...[W]e felt that without that level of transparency, there was no incentive for the officials to get on with the job and fix the problem.

Frankly, our view was that if the public was made aware on a regular basis, say twice a year, with the appropriate delays that we're suggesting, that there would be a level of outrage amongst the population that they're being forced to go through this long and cumbersome process, if it's only working 80 percent of the time, and we think that would be

²³¹⁴ Exhibit P-172, p. 81 of 155.

²³¹⁵ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4673.

²³¹⁶ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5050; Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5284.

²³¹⁷ Exhibit P-172, p. 81 of 155.

²³¹⁸ Exhibit P-172, p. 81 of 155.

²³¹⁹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5050.

a significant incentive to improve the system, to perfect the system. We don't ever expect a perfect system but we think that there should be some form of pressure on it and we don't see why just a select group of officials should be the only people that know how often the system fails.²³²⁰

Duguay disagreed with this approach, arguing that the risk of alerting terrorists to potential vulnerabilities outweighed the benefits of greater public awareness. He said that the failures identified by intrusion tests were better addressed through a quality assurance model which relied on oversight measures such as remedial training.²³²¹

How to disseminate important security information to the most appropriate recipients is an ongoing issue. Transport Canada, in a briefing to Commission staff, noted that the GA sector,²³²² among the weakest security links,²³²³ receives security advisories that are not necessarily provided to the commercial carriers. Transport Canada indicated that this was to prevent the undue alarm that can arise when too many people are provided with too much information. A balance was required so that the "...appropriate information reaches the appropriate people,"²³²⁴ according to the threat. It was essential that this balancing also consider the risks that too much emphasis on secrecy could cause, as occurred with the lack of information provided to air carriers whose passengers were interlined to Air India in June 1985. Had CP Air known of Air India's heightened threat environment, it is almost certain that the request to interline the "M. Singh" bag without the passenger having a reservation on Air India Flight 182 would have faced greater scrutiny. Similarly, important information about security threats and measures needs to be shared with the public in a manner that promotes overall security.

Transport Canada officials advised the Commission that the Department followed a policy of keeping the public informed about security measures, and was able to do so effectively without compromising national security.²³²⁵ The threat posed by liquid and gel explosives in August 2006 was cited as an example. An extensive public awareness campaign informed passengers about new pre-board screening (PBS) measures that had been developed, literally, overnight. Transport Canada and CATSA each quickly prepared information materials for air carriers and the public. Transport Canada officials recognized that the public needed information about the threat from liquid and gel explosives and about the additional security measures required at screening checkpoints.²³²⁶ This information was provided without giving away secrets that

²³²⁰ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4674.

²³²¹ Testimony of Yves Duguay, vol. 43, June 14, 2007, p. 5284.

²³²² The GA sector consists of private aircraft, including recreational aircraft, business aviation and specialty air services. See Exhibit P-101 CAF0827, p. 7 of 19.

²³²³ See Section 3.8.3, which discusses deficiencies in GA security.

²³²⁴ Exhibit P-101 CAF0827, p. 8 of 19.

²³²⁵ Testimony of Pierre Cyr, vol. 39, June 4, 2007, pp. 4826-4827.

²³²⁶ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4842.

could assist wrongdoers. For example, the public information did not include the type or amount of explosives necessary to damage an aircraft, “for obvious security reasons.”²³²⁷

Jean Barrette, Director of Security Operations for Transport Canada, stressed that the communications effort during the liquids and gels threat was merely one example of Transport Canada’s commitment to keeping the public informed about security issues. The Department had been “reaching out to the public,”²³²⁸ particularly since September 11, 2001, using a wide variety of materials to raise awareness about security measures and about the need to remain vigilant against terrorism.²³²⁹

Despite these assurances, the public may still not be sufficiently familiar with many security measures. Even when information is provided, it may not always be provided in a timely fashion. Terrorism breeds fear, and knowledge of some of the security measures in place to counter specific types of threats, such as those posed by liquids and gels, can provide reassurance to the travelling public. Superintendent Alphonse MacNeil, Officer in Charge of the Canadian Air Carrier Protective Program, which places covert in-flight security officers – commonly called “air marshals” – on select passenger aircraft, acknowledged that the Program needed to be better publicized, and that this could boost public confidence, while at the same time serving as a deterrent.²³³⁰ He testified that information could be shared with the public without jeopardizing national security interests: “[W]e want the Canadian travelling public to know that the air marshal program in Canada exists...and that we are on aircraft. We just can’t be specific about which aircraft.”²³³¹

Counsel for the Air India Victims’ Families Association asked witnesses to consider whether airlines could use their enhanced security as an advertising feature, particularly if a public warning system relating to threats against airlines were established. In fact, in 1985, because of persistent politically-related interference with civil aviation around the world, Wallis had considered whether airlines could develop a political risk analysis program for customers as a service to sell – a novel concept at the time.²³³² Whitaker agreed that airlines could use their security features as a selling point, similar to the way in which automobile manufacturers advertise safety features such as air bags. He stated that some airlines, such as Israel’s El Al, already do this, but that the decision to advertise security measures was for the air carrier to make.²³³³

Whitaker believed that the public was already aware of airlines that face greater risks, such as Air India and El Al, due to the heightened security measures

²³²⁷ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4842.

²³²⁸ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4843.

²³²⁹ Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4843.

²³³⁰ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, p. 8072.

²³³¹ Testimony of Alphonse MacNeil, vol. 65, October 24, 2007, pp. 8071-8072.

²³³² Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4295.

²³³³ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4612.

regularly used by these carriers. Passengers know to arrive at the airport for an El Al flight many hours earlier than is required for other airlines because of El Al's exhaustive screening process. Whitaker stated that "...those passengers presumably understand that, and accept that they're in effect buying better, greater security by undergoing a more intensive process."²³³⁴ This also demonstrates the challenge of balancing security with efficiency in air travel. Where there appears to be an increased risk, additional inconvenience may be both necessary and tolerated by passengers, particularly if they have been adequately educated about security issues.

Independent reporting is essential. The Commission commends the reviews of aviation security conducted by the CATSA Advisory Panel,²³³⁵ the Senate Committee²³³⁶ and the Auditor General of Canada.²³³⁷ Their work greatly facilitated the Commission's understanding of the current security weaknesses and strengths. Such reviews, particularly ongoing monitoring of the effectiveness of security by the Senate Committee and the Auditor General, must continue. Because of the ever-changing nature of air terrorism and the fact that gaps in civil aviation security remain poorly addressed, the Commission recommends a comprehensive, independent review of the Canadian civil aviation security regime every five years, similar to that carried out by the CATSA Advisory Panel. This will increase the accountability of the Government and help to keep the public adequately informed about security matters.

3.9.3 Conclusion

The aviation security experts and stakeholder representatives who appeared before the Commission largely opposed introducing a duty to warn the public about threats against airlines. Such a duty was considered impractical and open to abuse by terrorists and others wishing to cause disorder. A duty to warn could effectively shut down an airline.

It was also not considered appropriate for government to assume responsibility for warning the public, particularly about speculative threats. Only exceptional circumstances could warrant a public warning, and the appropriate threshold was difficult for experts to articulate. Further study is required to determine how the Government could discharge this duty in a manner that would enhance the security and confidence of the travelling public and respect commercial interests. Among the issues that should be examined are the policy and legal implications of a duty to warn, such as liability to affected airlines, commercial consequences and the appropriate threshold at which the public should be warned. The concept of a duty to warn is appealing, but its application could be problematic.

²³³⁴ Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4606.

²³³⁵ Exhibit P-169.

²³³⁶ Exhibits P-171 and P-172.

²³³⁷ Exhibit P-173.

In general, greater transparency is required in aviation security to bolster confidence in the system, to ensure that resources are being allocated effectively and to make certain that government and industry stakeholders remain accountable for managing their security mandates. A more appropriate balance between secrecy and keeping the public sufficiently informed is required.

Some aviation security experts opposed disclosing the results of intrusion tests to the public because of concerns about the release of sensitive security information. Others said that a limited degree of disclosure, including actions taken to address weaknesses, could increase public confidence in the Canadian aviation security system. Public release of such security records could also provide an incentive for deficiencies to be addressed in a timely and effective manner.

After carefully weighing the risks of alerting terrorists to potential vulnerabilities against the benefits of greater public awareness, the Commission does not recommend the publication of intrusion test results. If a decision is nonetheless made to publish results, publication should only occur after passage of sufficient time to enable the specific vulnerabilities in the system to be addressed.

Independent reporting by bodies such as the Senate Committee and the Auditor General of Canada must continue. Given the dynamic nature of civil aviation security and the Government's record of delays in addressing security deficiencies, a formal, independent review of civil aviation security in Canada should take place every five years.

3.10 Funding Aviation Security

3.10.1 Cost-effective Security: Reasonable Balance, Flexibility and a Risk Management Approach

Measures designed to optimize civil aviation security must often be adjusted to meet the commercial needs of the aviation industry.²³³⁸ In 1985, the Seaborn Report recognized the tension between achieving good security and facilitating good business:

The threat of terrorism must not be permitted unduly to interfere with the normal activities of daily life, including air travel. It must, however, be recognized that air travellers are vulnerable to terrorist and other similar attacks. It is, therefore, most important that air security be based on efficient as well as effective means, as a matter of routine, of security checking large numbers of persons and their baggage as well as air

²³³⁸ Achieving good security and facilitating business are two components of the security "triangle," the third being respect for the rights and values of Canadians. See Testimony of Jean Barrette, vol. 40, June 5, 2007, p. 4893.

cargo and mail. As the threat increases more painstaking checks become necessary, resulting in proportionately more inconvenience to the travelling public. The key points, however, are to ensure a basic standard of security whose diligent application will satisfy the need to operate the air system both efficiently and safely....²³³⁹

Commissioned in the wake of the Air India bombings, the report noted the "... need for a reasonable balance between the expeditious movement of passengers and the assurance of their safety and security."²³⁴⁰ It stressed the importance of "...practical means of improving airport and airline security."²³⁴¹ This approach continues today.²³⁴² Annex 17 to the *Convention on International Civil Aviation* ("*Chicago Convention*") requires effective aviation security and efficient air travel to be accomplished together.²³⁴³

The tension between security and efficiency often surfaces in discussions of cost and convenience. Government and industry resources are finite and security measures can be expensive. In 1985, the cost of security measures and the customer service interests of private industry played a role in Air India's decision to use ineffective technology to screen checked baggage instead of relying on passenger-baggage matching procedures. Manual methods of passenger-baggage matching were known to prevent bags from travelling without their corresponding passengers in circumstances of high threat, but were time-consuming and inconvenient.²³⁴⁴ At the time, passenger and baggage screening was the responsibility of air carriers. As profit-seeking entities, the carriers would not rank security as their primary concern.²³⁴⁵ However, Transport Canada knew about the decision to reject passenger-baggage matching measures.²³⁴⁶ The evidence points to the conclusion that, in 1985, given the threat facing Air India, costs and passenger convenience were not "reasonably balanced" with security.

The concerns of private industry must not override necessary and otherwise appropriate security measures. However, those monitoring civil aviation security have suggested that this does occur and that it has led to serious gaps in aviation security. Dr. Kathleen Sweet, an international civil aviation security consultant, contended that considerable industry lobbying against new air cargo security requirements in the US resulted in a delay in implementing important

²³³⁹ Exhibit P-101 CAF0039, p. 10 of 10.

²³⁴⁰ Exhibit P-101 CAF0039, p. 2 of 10.

²³⁴¹ Exhibit P-101 CAF0039, p. 2 of 10.

²³⁴² Exhibit P-169, p. 23 of 202.

²³⁴³ Contracting States are required to "establish and implement a written national civil aviation security programme to safeguard civil aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights": Exhibit P-181, p. 3-1, s. 3.1.1.

²³⁴⁴ Exhibit P-101 CAF0581, pp. 1-2; see also Exhibit P-101 CAF0637, pp. 14-15.

²³⁴⁵ Exhibit P-157, p. 67 of 135.

²³⁴⁶ Exhibit P-101 CAF0581, pp. 1-2.

new measures. Passenger airlines, all-cargo carriers and freight forwarders complained that the measures were too costly. Sweet noted, however, that despite significant air cargo scanning requirements, air carriers in Europe and Asia managed to remain profitable.²³⁴⁷

Concerns that security has been sacrificed for efficiency have also been raised in Canada. In its 2003 report, *The Myth of Security at Canada's Airports*, the Standing Senate Committee on National Security and Defence (Senate Committee) recommended that cargo and mail be fully screened.²³⁴⁸ Still, cargo and mail do not undergo routine screening today in Canada,²³⁴⁹ even though both were recognized as vulnerable to sabotage as early as 1980. In a formal response to the Senate Committee's recommendation, Transport Canada acknowledged the vulnerability of air cargo, stating that the Department had begun policy discussions with stakeholders and that pilot projects were planned to mitigate risks and to facilitate "...the efficient movement of goods domestically and globally."²³⁵⁰ Facilitating the free flow of commerce is a stated objective of Transport Canada's proposed Air Cargo Security (ACS) Initiative.²³⁵¹ The Senate Committee was critical of the length of time taken to enhance air cargo security and was troubled by the possibility that concerns about efficiency were trumping security concerns.²³⁵²

Transport Canada officials explained that cost is "always an issue"²³⁵³ when developing aviation security measures, but that the most relevant concern was the safety and security of passengers.²³⁵⁴ Transport Canada consults with stakeholders, most often airports and air carriers, who ultimately implement the regulatory requirements. Advice from stakeholders about cost implications "...helps enable the department to carry out a full assessment of costs against security benefits...and to inform decisions about whether...proposed security requirements should be adjusted or should be changed in any way."²³⁵⁵

There is no doubt that costs must be contained, but experts and stakeholders who appeared before the Commission were resolute that cost-effective security measures were attainable and that delays in implementing important security measures were unnecessary. Sweet testified that good security did not have to be costly:

...[Y]ou need to have things in place on the ground that [are] preventive in nature...that are common sense and do not cost a fortune. I think there are so many smaller things that can be done to protect the terminals, the airport facilities, and the

²³⁴⁷ Lufthansa and Singapore Airlines were specifically cited: Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4948-4949.

²³⁴⁸ Exhibit P-171, p. 59 of 256.

²³⁴⁹ Exhibit P-169, pp. 52-53 of 202.

²³⁵⁰ Exhibit P-172, pp. 41-42 of 155.

²³⁵¹ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5184.

²³⁵² Exhibit P-172, pp. 42-43 of 155.

²³⁵³ Testimony of Jean Barrette, vol. 38, June 1, 2007, p. 4567.

²³⁵⁴ Testimony of Jean Barrette, vol. 38, June 1, 2007, p. 4567.

²³⁵⁵ Testimony of Jim Marriott, vol. 38, June 1, 2007, p. 4566.

aircraft before it takes off, that are not really sufficiently being utilized. There are certain technological things that obviously we need to be using because technology helps us in many areas, but I just don't agree with the concept that technology is the saviour of aviation security. It isn't, it's a component. It's another tool in the tool box and it needs to be used appropriately and I don't think that any country in the world frankly is using every tool in the tool box.²³⁵⁶

Sweet gave the example of explosives detection dogs as a less costly measure than advanced technology for cargo screening. Although dogs had limited attention spans and needed frequent rests, they were inexpensive and highly effective, at least for random cargo screening:

...[W]ith those big cargo pallets, you use dogs. Incredibly, \$10,000 to train them; they'll last for a good 10 to 12 years. Have a good trainer -- a good handler, and that dog is good. Those dogs are good. You know, they can sniff out...5,000 to 7,000 different chemicals, organic compounds or more. Use dogs.²³⁵⁷

Rodney Wallis, an expert in international civil aviation security, agreed that good security could be economical and did not always require expensive technology. He testified that many developing countries cannot afford the most advanced technology and that "...[p]robably the most effective security is when you are using people, properly managed, at very low costs. And so there is no reason why most security issues in the [East] couldn't be handled as effectively as they are in the West."²³⁵⁸ He stated, however, that technology was required to handle large volumes of passengers.²³⁵⁹ He agreed that well-trained dogs were an inexpensive and effective alternative for cargo screening, particularly where resources are constrained. However, he testified that relying solely on dogs in a major facility was not a viable option. The volume of cargo traffic made the use of technology unavoidable.²³⁶⁰

Wallis testified that having the flexibility to match available resources to security needs was essential in civil aviation security.²³⁶¹ For example, passenger-baggage reconciliation could be achieved by a variety of methods.²³⁶² Where there are greater resources, automated systems may be an option, but where resources are more limited, manual systems of reconciliation could be equally effective.

²³⁵⁶ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4940-4941.

²³⁵⁷ Testimony of Kathleen Sweet, vol. 41, June 6, 2007, pp. 4954-4955.

²³⁵⁸ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4292.

²³⁵⁹ Testimony of Rodney Wallis, vol. 36, May 30, 2007, p. 4292.

²³⁶⁰ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5007.

²³⁶¹ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5007.

²³⁶² Exhibit P-101 CAF0827, p. 16 of 19.

Performance-based or results-oriented security measures, in which the desired outcome is prescribed but the method for achieving it is not,²³⁶³ are essential if civil aviation security is to have the flexibility it needs. This flexibility promotes the use of cost-effective measures. Following the bombing of Air India Flight 182, the regulatory framework for aviation security in Canada became much more prescriptive. Detailed regulations were adopted for such procedures as passenger-baggage reconciliation. The prescriptive regulatory approach was reinforced after the events of September 11, 2001.²³⁶⁴

Can a regulatory approach with such an important goal become too prescriptive? According to the CATSA Act Review Advisory Panel (CATSA Advisory Panel), the regulatory framework, at least as it applied to the Canadian Air Transport Security Authority (CATSA), was overly prescriptive. It spelled out "...in the most minute fashion specifically what has to be done, and by whom, in a certain set of circumstances, as well as the manner in which to do it."²³⁶⁵ The *Security Screening Order*, which provided instructions to CATSA on how to conduct its screening responsibilities,²³⁶⁶ was extremely detailed, leaving little room for CATSA to make operational decisions, deploy resources efficiently or develop innovative ways to attain its goals.²³⁶⁷

The CATSA Advisory Panel found that budgetary constraints placed on CATSA as a government organization could also affect security screening performance. For example, budgets could not be adjusted easily to changes in passenger volume.²³⁶⁸ The Panel also observed that terrorist efforts to evade existing security measures put pressure on the aviation security regime to be able to predict the nature of future attacks, assess risks, set priorities and devise workable solutions.²³⁶⁹ It further noted that the current prescriptive regulatory framework for CATSA might be more costly and less efficient to operate, particularly when flexibility was required.²³⁷⁰

The Panel stated that, with limited resources and the costliness of some security measures, decisions must be made on a sound risk-assessment basis.²³⁷¹ Smaller airports with little traffic and less risk, for example, were subjected to the same security screening requirements as larger Class 1 airports. Such inflexibility in the system could be costly for both CATSA and smaller airports. The Panel suggested that if security were maintained in a more flexible manner based on risk assessment, more stringent requirements could be warranted for Class 1 airports, while alternative and cost-effective measures could be used at smaller airports. The Panel noted that this had been done with security measures in

²³⁶³ Exhibit P-101 CAF0827, p. 16 of 19.

²³⁶⁴ Exhibit P-169, p. 91 of 202.

²³⁶⁵ Exhibit P-169, p. 91 of 202.

²³⁶⁶ Exhibit P-157, p. 114 of 135.

²³⁶⁷ Exhibit P-169, p. 91 of 202.

²³⁶⁸ Exhibit P-169, p. 104 of 202.

²³⁶⁹ Exhibit P-169, p. 155 of 202.

²³⁷⁰ Exhibit P-169, p. 91 of 202.

²³⁷¹ Exhibit P-169, p. 155 of 202.

areas other than screening. It concluded that providing CATSA with greater flexibility in its screening operations at some smaller airports could reduce costs and enable resources to be deployed to higher-volume airports, improving service for the travelling public without compromising security.²³⁷²

An overly prescriptive regulatory framework can increase security risks. Mandatory and highly standardized security procedures can easily become predictable. This enables those who observe the system for long enough to circumvent it. Such procedures may also mean that new equipment or measures are adopted less quickly. An environment of changing threats to civil aviation security requires the system to be able to respond.²³⁷³ The CATSA Advisory Panel recommended that Transport Canada make it a high priority to develop an approach to regulation and compliance monitoring that was more performance-based and results-oriented than the existing regulatory model.²³⁷⁴

Transport Canada has indicated that it favours a more performance-based approach, after having received feedback from stakeholders during the Aviation Security Regulatory Review.²³⁷⁵ The stated purpose of the review was to renew the structure of the aviation security regulatory framework, its approach and its content.²³⁷⁶ Between January and April 2008, Transport Canada held briefings with stakeholders across Canada to introduce them to the review. Feedback included a call for flexibility in the regulatory regime, and a recognition that the industry was diverse and that change must be manageable. However, Transport Canada also reported that the aviation industry at times preferred a prescriptive approach from a business perspective because costs were then more predictable.²³⁷⁷

As an example, Stephen Conrad of Transport Canada explained that one key objective of the Department's proposed initiative to enhance air cargo security was to use a performance-based regulatory approach. The Department recognized, however, that some prescriptive regulations were needed as well.²³⁷⁸ Again, balance was required. In 1985, the bombing of Air India Flight 182 occurred under a broadly performance-based regulatory framework.²³⁷⁹ There was little guidance, and required outcomes were vaguely stated. For the proposed Air Cargo Security Initiative, Conrad testified that Transport Canada believed a blend of approaches to be necessary:

From a regulatory approach, there's been some discussions about performance based versus prescriptive regulations, and,

²³⁷² Exhibit P-169, p. 96 of 202.

²³⁷³ Exhibit P-169, p. 92 of 202.

²³⁷⁴ Exhibit P-169, pp. 92-93 of 202.

²³⁷⁵ Exhibit P-101 CAF0827, p. 16 of 19.

²³⁷⁶ The scope of the review included identifying legislative issues and amendments necessary for the *Aeronautics Act* and the *CATSA Act* and all the corresponding regulatory instruments, including Measures, Orders and Alert Condition and Response Systems: Exhibit P-101 CAF0835, pp. 6-7 of 35.

²³⁷⁷ Exhibit P-101 CAF0827, p. 17 of 19.

²³⁷⁸ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5185.

²³⁷⁹ Exhibit P-169, p. 91 of 202.

in our view, you need some of both. We are moving through security management systems to more performance based regulations, but there will always be a need in certain areas where it's either very technical or very complex where you need to be prescriptive in certain areas but making sure that we have the right balance to allow flexibility and industry to come up with unique and innovative ways of solving new and emerging problems.²³⁸⁰

Outcomes need to be prescribed in detail, and greater prescription may be required about the methods to achieve them. Vigilant regulatory oversight will assist in ensuring adequate compliance. Flexibility, including a balance between prescriptive and performance-based regulatory approaches, promises to bring cost-effective solutions to civil aviation security problems.

Adherence to good risk management decision-making principles²³⁸¹ will also assist in achieving the right balance between security and efficiency. Risk management decision-making has, as an express objective, the best allocation of risk control budgets in the most cost-effective manner possible.²³⁸² Appropriate risk management practices assess and rank all risks according to a systematic protocol in order to distribute finite resources:

Managing the risks for which one is responsible costs money. Since resources are always constrained, an institution's "risk budget" must be allocated across the full set of risks in some defensible scheme. The principle of cost-effectiveness (maximum benefit per unit of expenditure) can be used here, with the proviso that no important risk can be short-changed: In other words, both public expectations and good business practices demand that corporations and governments should control specified risks to a level that is regarded as "acceptable."²³⁸³

Dr. William Leiss, an expert in risk management retained by the Commission, argued that cost-effective risk management practices needed to be implemented, not only by government, but by all stakeholders involved in civil aviation security, using common methods based on current best practices that are understood by all, since this mandate is a shared responsibility.²³⁸⁴ Concerted and complementary efforts by all entities would help keep civil aviation security costs manageable. The consultations that occurred when security measures were being developed²³⁸⁵ could contribute to this process. In

²³⁸⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, pp. 5185-5186.

²³⁸¹ See Section 3.3 for a complete review of risk management decision-making in civil aviation security.

²³⁸² Exhibit P-361, Tab 1, p. 3.

²³⁸³ Exhibit P-361, Tab 1, p. 9.

²³⁸⁴ Exhibit P-361, Tab 1, p. 8.

²³⁸⁵ Testimony of Jim Marriott, vol. 38, June 1, 2007, p. 4566.

addition, discussions about cost-effective security measures should take place during regular meetings of the Advisory Group on Aviation Security (AGAS) and its Technical Committees and Working Groups.²³⁸⁶

However, there is reason to doubt that systematic risk management practices have thus far been employed to assess all risks²³⁸⁷ or that stakeholders have harmonized these processes.²³⁸⁸ A 2005 report of the Auditor General of Canada that reviewed the government's 2001 Anti-Terrorism Initiative recommended that Transport Canada conduct "...a formal analysis of threats and risks to the entire air transport system"²³⁸⁹ and that it use the results as the basis for deploying resources.²³⁹⁰ Transport Canada developed a formal risk assessment methodology in 2006.²³⁹¹

Effective risk management procedures should ensure that the security system has no gaps.²³⁹² However, the CATSA Advisory Panel found that critical gaps remain in areas such as air cargo and access to airside and restricted areas of airports, and that these continue to expose passengers to considerable risk of sabotage.²³⁹³ Transport Canada has proceeded with measures designed to enhance passenger and baggage screening.

Wallis criticized the Passenger Protect Program, the Canadian "no-fly" list initiated in June 2007.²³⁹⁴ Citing the many difficulties experienced with the US no-fly list, Wallis questioned the rationale and effectiveness of the Canadian Program and, consequently, the value of diverting limited resources to it:

And since we know all the problems that have been associated with [the American] list, I really do wonder why one would push ahead with the particular program here. I don't see the value of it.

...

...[I]t's going to cost money. It probably has cost a lot of money [already] to get this far, but it's going to cost money to manage and I think that there is always a limit on resources available in any line of work, and it seems to me that money is being misspent, misused and it could be used better perhaps in pushing ahead on one of the other areas of security that requires action now.²³⁹⁵

²³⁸⁶ Exhibit P-101 CAF0859, pp. 2-3 of 44.

²³⁸⁷ See, for example, Testimony of William Leiss, vol. 91, December 7, 2007, p. 11990.

²³⁸⁸ Exhibit P-101 CAF0873, p. 4 of 6.

²³⁸⁹ Exhibit P-411, p. 9.

²³⁹⁰ Exhibit P-411, p. 9.

²³⁹¹ Exhibit P-101 CAF0873, p. 3 of 6.

²³⁹² Exhibit P-361, Tab 1, p. 9.

²³⁹³ Exhibit P-169, pp. 68-69 of 202.

²³⁹⁴ Exhibit P-278, Tab 15, p. 1.

²³⁹⁵ Testimony of Rodney Wallis, vol. 41, June 6, 2007, p. 5021.

This discussion of costs must take into account another major cost – that of aviation security incidents.

3.10.2 Sustainable Funding

Resources are finite even in times of budgetary surplus. Regardless of the economic situation, funding for aviation security must be sufficient to cover all important risks and provide an acceptable level of overall security. In other words, funding must be sufficient to achieve an acceptable level of overall risk. Security gaps remain in air cargo,²³⁹⁶ Fixed Base Operations (FBOs) and the General Aviation (GA) sector,²³⁹⁷ as well as in secure and public areas of airports.²³⁹⁸ Clearly, an acceptable level of overall risk has not been achieved. Resources are now too heavily weighted towards passengers and their baggage,²³⁹⁹ leaving other significant vulnerabilities.

A civil aviation security regime that adequately addresses all risks during normal threat levels and that can respond to heightened levels of threat requires sustained funding over time. Following the events of September 11, 2001, the federal Budget allotted \$2.2 billion over a five-year period to enhance aviation security. The Government also introduced the Air Travellers Security Charge (ATSC), paid by air travellers beginning in April 2002. The *Air Travellers Security Charge Act*²⁴⁰⁰ created the ATSC to fund several aviation security initiatives, including:

- An enhanced regulatory regime;
- Additional Transport Canada security inspectors;
- The installation of cockpit doors on passenger aircraft;
- Increased policing presence at airports;
- The establishment of the RCMP's Canadian Air Carrier Protective Program (CACPP); and
- The creation of CATSA for passenger and baggage screening.²⁴⁰¹

Of the \$2.2 billion provided in the 2001 Budget, 88 per cent was allocated to the last three initiatives.²⁴⁰²

The Government's intention was for ATSC revenues to cover the expenditures required for the enhanced security initiatives over a five-year period. However, the Commission learned that there was no direct link between the ATSC collected and subsequent security expenditures. The ATSC is managed by the Department

²³⁹⁶ Exhibit P-169, p. 52 of 202.

²³⁹⁷ Exhibit P-169, p. 55 of 202.

²³⁹⁸ Exhibit P-169, pp. 57, 69-70.

²³⁹⁹ Exhibit P-411, p. 9.

²⁴⁰⁰ S.C. 2002, c. 9, s. 5.

²⁴⁰¹ Exhibit P-169, p. 168 of 202.

²⁴⁰² Exhibit P-169, p. 168 of 202.

of Finance, and revenues flow directly into the Consolidated Revenue Fund. Aviation security expenditures, including those related to CATSA's operations, are set by parliamentary appropriations.²⁴⁰³ Because of the inability to track ATSC funds once they are collected, stakeholders expressed little confidence that ATSC revenues were ultimately or entirely invested in aviation security.²⁴⁰⁴

Most aviation industry stakeholders, including the Canadian Airports Council (CAC), the Air Transport Association of Canada (ATAC),²⁴⁰⁵ the Air Line Pilots Association, International (ALPA),²⁴⁰⁶ airport authorities and air carriers²⁴⁰⁷ were strongly opposed to the ATSC. They argued that the ATSC lacked transparency, comprehensive accounting and appropriate investment in the air transportation industry.²⁴⁰⁸ They also complained that the security charge unfairly penalized the aviation sector, while other modes of transportation that could equally be targeted by terrorists were not subject to a comparable charge.²⁴⁰⁹ Most significantly, as Captain Craig Hall, Director of the National Security Committee of ALPA, argued, civil aviation security was a national security issue and the federal government should bear all costs:

...[W]hether we're talking about 9/11; whether we're talking about Air India; whether we're talking about Pan Am 103; whether we're talking about any one of these absolutely horrible acts...the attack was not against aviation.

The attack was not against the people who were on the aircraft; it was not against the air carrier; it was not against the buildings in the case of 9/11. The attack was a fundamental attack on our way of life; on the things we hold dear as a nation and as a people. That...falls under the heading of national security and we believe that funding for security needs to be borne by the federal government just the way that the federal government funds [our] national policing force...exactly the same way that the federal government funds our armed forces.

And it should not be put on the traveling public in terms of punitive air travelers security charges which are...totally inappropriate...It's a national security issue. It should be supported by the federal government.²⁴¹⁰

Who should pay for aviation security has long been the subject of debate. In the 1980s, the International Air Transport Association (IATA) argued that airlines should not pay for security measures because the government was the real

²⁴⁰³ Exhibit P-169, pp. 168-169 of 202; see also Testimony of Pierre Cyr, vol. 39, June 4, 2007, p. 4798.

²⁴⁰⁴ Exhibit P-169, p. 172 of 202.

²⁴⁰⁵ Exhibit P-169, p. 169 of 202.

²⁴⁰⁶ Testimony of Craig Hall, vol. 64, October 23, 2007, p. 8004.

²⁴⁰⁷ Exhibit P-169, p. 169 of 202.

²⁴⁰⁸ Exhibit P-169, p. 169 of 202.

²⁴⁰⁹ Exhibit P-169, p. 174 of 202.

²⁴¹⁰ Testimony of Craig Hall, vol. 64, October 23, 2007, pp. 8003-8004.

target when an aircraft was attacked. The attraction of the aircraft lay in the national flag it carried on its tail, so that "...you have got a small piece of your target country,"²⁴¹¹ the primary aim of terrorists:

Acts of terrorism of the type experienced by civil aviation in the mid/late 1980s are unquestionably political in their concept. They are certainly carried out by clandestine political organizations who see their actions as being directed against states. The object of the attack is an aircraft but an aircraft seen to represent the government of registry, not the shareholders of the company.²⁴¹²

Wallis testified similarly that attacking an airport terminal in a target country sends a powerful political message.²⁴¹³

The CATSA Advisory Panel responded to arguments that government should bear the cost of civil aviation security by noting that air travellers and the civil aviation industry were the primary beneficiaries of aviation security measures and should therefore pay the associated costs. Enhanced security measures also provided a significant economic benefit to the aviation industry, without which consumers might choose other modes of transportation, potentially reducing the economic viability of some air carriers. The Panel argued that the cost of funding security measures must be seen as a cost of doing business in civil aviation.²⁴¹⁴ It also argued that the ATSC represented a small fraction of the additional fees that air passengers paid when they bought tickets, and that this had a marginal impact on their purchasing decisions.²⁴¹⁵

The CATSA Advisory Panel reviewed the arguments about the ATSC and concluded that imposing a separate charge for security initiatives accorded with international practice and was not unreasonable. In the US, passengers and air carriers both pay security fees. In 2005, such fees allowed the Transportation Security Administration (TSA) to recover about 43 per cent of its security expenses. In Europe, security operations are funded by a combination of stakeholders, including airports, air carriers and passengers, as well as by the states themselves.²⁴¹⁶ The CATSA Advisory Panel recommended an annual public reporting about the ATSC. The Panel concluded that transparency could be improved by showing expenditures by program or department. Reporting capital expenditures as they were appropriated, rather than on a depreciation basis, would also be useful.²⁴¹⁷ The Senate Committee also recommended a

²⁴¹¹ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4243.

²⁴¹² Wallis, *Combating Air Terrorism*, p. 1.

²⁴¹³ Testimony of Rodney Wallis, vol. 35, May 29, 2007, p. 4244.

²⁴¹⁴ Exhibit P-169, p. 171 of 202.

²⁴¹⁵ The Panel provided the following example: a \$415 return ticket between Ottawa and Toronto would cost a passenger \$70 in fees and charges, including the ATSC. Out of a total price of \$485, an ATSC of \$9.90 represents approximately 2 per cent of the cost: Exhibit P-169, p. 171 of 202.

²⁴¹⁶ Exhibit P-169, p. 172 of 202, note 5.

²⁴¹⁷ Exhibit P-169, p. 174 of 202.

detailed accounting of how and where the ATSC was collected and spent,²⁴¹⁸ including itemized revenues and expenditures by airport and an annual government report on the appropriateness of the amount charged.²⁴¹⁹

Stakeholders agreed that, if the ATSC were retained, there must be full transparency about how the funds are distributed and the funds generated should be used exclusively for the aviation industry, not for other modes of transportation.²⁴²⁰ They argued that all or part of the ATSC should be credited to CATSA's appropriations, which would directly link CATSA's funding to passenger growth and related workload increases.²⁴²¹ Surpluses could be used to fund additional screeners and improved equipment and to compensate airports for lost commercial opportunities because of the space requirements for pre-board screening (PBS) checkpoints.²⁴²²

Both the CATSA Advisory Panel and the Senate Committee noted that the ATSC had dropped significantly since its introduction. In 2002, the ATSC paid by travellers was \$24 for domestic, continental and international round trip flights.²⁴²³ The ATSC was progressively reduced in the federal budgets of 2003, 2004 and 2005. By 2006, the ATSC dropped to \$9.90 for domestic, \$16.84 for continental and \$17.00 for international round trip flights.²⁴²⁴ As of April 2009, these figures were \$9.80, \$16.68 and \$17.00 respectively.²⁴²⁵ The CATSA Advisory Panel reported that reductions were a result of consultations with stakeholders, reports by independent consultants, revised forecasts in the growth of air passenger traffic, CATSA annual reports revealing unspent operating funds and consecutive revenue and expenditure assessments.²⁴²⁶ According to the Senate Committee, however, the incremental reductions in the ATSC gave the impression that the Government was collecting more than it needed to fund aviation security.²⁴²⁷ The Committee observed that only about 25 per cent of the improvements required in airport security had been completed by 2007. It questioned whether the ATSC should be decreasing if the delay in completing the improvements was a cost issue.²⁴²⁸

The Government has since decided to retain the ATSC to fund security initiatives, to use surpluses to offset increased operating costs and to fund some future capital expansions. It has also decided to review and report on the ATSC periodically.²⁴²⁹

²⁴¹⁸ Exhibit P-172, pp. 86, 105 of 155.

²⁴¹⁹ Exhibit P-172, p. 88 of 155.

²⁴²⁰ See, for example, Testimony of Fred Jones, vol. 65, October 24, 2007, p. 8139.

²⁴²¹ Exhibit P-169, p. 174 of 202.

²⁴²² Exhibit P-169, p. 174 of 202.

²⁴²³ This figure was inclusive of the excise tax (the GST or the federal portion of the HST), as applicable under s. 165(1) of the *Excise Tax Act*. See Exhibit P-172, p. 83; see also Exhibit P-169, p. 170 of 202.

²⁴²⁴ Exhibit P-172, p. 84 of 155.

²⁴²⁵ See *Air Travellers Security Charge Act*, S.C. 2002, c. 9, s. 5, ss. 12(1), 12(2).

²⁴²⁶ Exhibit P-169, p. 168-169 of 202.

²⁴²⁷ Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4676.

²⁴²⁸ Exhibit P-172, p. 84 of 155; see also Testimony of Colin Kenny, vol. 38, June 1, 2007, p. 4676.

²⁴²⁹ Exhibit P-169, p. 174 of 202.

Initiatives to address current gaps in aviation security will require initial and ongoing funding. With Transport Canada's proposed Air Cargo Security (ACS) Initiative, for example, the Department was considering funding options, including whether funding from government or industry or through user-pay models would best ensure sustainability of the program.²⁴³⁰ Moses Aléman, an expert in civil aviation security, noted that air cargo on passenger flights is a significant source of revenue for most airlines in the world – so much so that many airlines would go bankrupt without it.²⁴³¹ Conrad testified that a user-pay model would be likely. For air cargo, this would mean that most of the additional costs would fall to the shipper, as the end-user.²⁴³²

Based on the evidence available to it, the Commission has concluded that civil aviation security is a core part of national security. For this reason, funding must come primarily from government. But civil aviation security is also a shared responsibility. Where reasonable and necessary, other sources of funding, including industry and end-user fees, can and should be sought. If funding comes from non-governmental sources, a meticulous accounting analysis that clearly traces the collection and expenditure of funding should be publicly available.

3.10.3 Conclusion

It is important to strike a reasonable balance between optimal security and a viable air travel industry. The evidence suggests that good risk management practices and operational flexibility can both facilitate economical solutions and enhance security. Key to cost-effective aviation security is a regime based on best practices in risk management, whose objective is to allocate limited resources in a manner that minimizes overall risk. The flexibility realized through a more performance-based, results-oriented approach not only assists in responding to the changing threats in civil aviation security, but can also help in reducing costs. However, just as an overly prescriptive regime can lessen security, so too can one that is overly performance-based. A balance is required here as well. Rigorous regulatory oversight must be in place to ensure compliance with specific security objectives.

Regular, sustained funding is required to maintain security at an acceptable level. Governments must be vigilant in times of fiscal restraint to ensure a level of funding that reflects the seminal importance of aviation security. While funding may require a mix of sources, including government, industry and users, decisions about funding are ultimately political. No matter which approach is taken, it must be principled, transparent and consistent.

²⁴³⁰ Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5186.

²⁴³¹ Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4246.

²⁴³² Testimony of Stephen Conrad, vol. 42, June 13, 2007, p. 5201.

Epilogue

The recommendations in this volume address current threats to aviation security, but those threats are constantly evolving. Additional security measures not contemplated by these recommendations may be required in future. An incident that occurred after this volume was completed illustrates this.

On December 25, 2009, a Northwest Airlines aircraft en route from Amsterdam to Detroit narrowly escaped disaster when a passenger failed in his attempt to detonate explosives. He had managed to board in Amsterdam with the explosives hidden in his underwear. He apparently tried to detonate the explosives as the aircraft approached Detroit. A small fire resulted, but there was no explosion. Other passengers and the crew subdued him and the aircraft landed safely.

US President Barack Obama immediately ordered an inquiry. The inquiry report revealed significant security failures:

...[T]he US government had the information – scattered throughout the system – to potentially uncover this plot and disrupt the attack. Rather than a failure to collect or share intelligence, this was a failure to connect and understand the intelligence that we already had.²⁴³³

The Government of Canada responded to the Northwest Airlines incident. In a January 5, 2010, news release the Government announced that it would introduce full body scanners at major Canadian airports as a voluntary screening alternative for passengers who did not want to undergo a physical search.²⁴³⁴ The body scanner is said to enhance the ability to detect articles hidden under clothing. The release stated that the Government would soon issue a “request for proposal” for passenger-behaviour observation in screening at major Canadian airports.

The news release did not discuss the central issue in the December 25 incident: the failure of the US government to process the intelligence it held about the passenger that might have led to his apprehension before he boarded the aircraft.

The Northwest Airlines incident illustrates the point, made in Volume One, that terrorist threats are constantly evolving and so require flexibility in security measures. Attempts by suicidal passengers to destroy aircraft have occurred

²⁴³³ The White House, Office of the Press Secretary, Remarks by the President on Strengthening Intelligence and Aviation Security, January 7, 2010: <http://www.whitehouse.gov/the-press-office/remarks-president-strengthening-intelligence-and-aviation-security>.

²⁴³⁴ Transport Canada, News Release, “Government of Canada invests in full body scanners and behaviour screening to further enhance security at Canadian airports”: <http://www.tc.gc.ca/eng/mediaroom/releases-2010-h002e-5794.htm>.

before, but the method used in this incident to hide explosives was new. The changing threat environment highlights the importance of a multi-layered approach to security so that an individual who evades detection by one layer can be caught by another. Unfortunately, this incident also shows that, even with a multi-layered approach, absolute security is almost impossible to achieve. Imperfect application of layers of security – such as inadequate intelligence-sharing and analysis, or passenger screening – can combine to create dangerous vulnerabilities. It was mere good fortune that the explosive device carried by the Northwest Airlines passenger did not detonate with tragic consequences.

VOLUME FOUR AVIATION SECURITY

CHAPTER IV: RECOMMENDATIONS

I. Oversight of Aviation Security in Canada

The Commission endorses the Government's decision that responsibility for national civil aviation security should remain with Transport Canada, and makes the following recommendations about oversight of aviation security:

Recommendation 1

1. Canada's regulatory regime must comply with the standards specified in Annex 17 to the *Convention on International Civil Aviation* ("*Chicago Convention*") and should comply with its recommended practices.
 - 1.1. Annex 17 standards must be considered minimum standards that Canada should not only meet, but exceed. Canada should not permit security deficiencies that would result in it being required to file a difference with the International Civil Aviation Organization (ICAO) with respect to any Annex 17 standard.
 - 1.2. In addition to embracing Annex 17 at its core, Canada's national regulatory regime must be informed by international best practices and must address Canada's unique threat environment.
 - 1.3. Transport Canada should exercise robust regulatory oversight over civil aviation stakeholders through regular inspection, testing, auditing and enforcement, carried out by a sufficiently trained, qualified and resourced inspectorate.

Recommendation 2

2. In accordance with Annex 17, Transport Canada should establish and implement a single, written National Civil Aviation Security Program that comprehensively safeguards civil aviation against acts of unlawful interference.
 - 2.1. The National Civil Aviation Security Program should set out the full slate of legislative instruments, measures, policies, practices and procedures, as well as the roles and responsibilities of Transport Canada, airport operators, air carriers, Fixed Base Operations (FBOs),

the General Aviation (GA) sector, the Canadian Air Transport Security Authority (CATSA), the police of local jurisdiction, airport tenants, caterers and all other entities involved in implementing the Program.

- 2.2. Transport Canada should require all entities with responsibilities in civil aviation security, as outlined in Recommendation 2.1, to establish and implement written security programs that are applicable to their operations and appropriate to meet the requirements of the National Civil Aviation Security Program. At a minimum, these programs should include measures to prevent unauthorized access, assign security-related duties, respond to threats and breaches of security, and allow for periodic review and updating of the programs.
- 2.3. Transport Canada should require all civil aviation stakeholder programs to be submitted to it for approval.

Recommendation 3

3. The Commission supports continued coordination between all industry and government entities responsible for civil aviation security through the Advisory Group on Aviation Security (AGAS). AGAS must continue to promote collaboration, shared objectives and shared understanding, and common solutions to aviation security problems.
 - 3.1. Transport Canada should require all airports to establish an airport security committee to help in implementing their respective airport security programs.
 - 3.2. Consideration should be given to the inclusion of the National Security Advisor (NSA) in AGAS discussions and decisions.

Recommendation 4

4. In addition to adhering to Annex 17 standards, a regulatory regime should observe a number of key principles:
 - a. Ongoing, informed assessment of past, present and future threats to civil aviation, with timely proactive adjustments made to the regime as needed;
 - b. Adherence to an appropriate national risk management protocol, as described in Recommendation 6;
 - c. Effective, multi-layered and overlapping security measures, policies, practices and procedures that provide redundancies to address all significant risks;

- d. A flexible, performance-based approach to regulation, in which objectives are set to meet the highest standards, with a more prescriptive approach employed where necessary because of complexities and context;
- e. Robust emergency response planning, with well-defined roles and responsibilities; and
- f. Establishment of a culture of security awareness and constant vigilance.

Recommendation 5

- 5. Independent experts should conduct a comprehensive review of aviation security every five years.

II. Risk Management

Recommendation 6

- 6. Transport Canada should ensure that acceptable levels of risk control have been achieved in all areas of risk pertinent to civil aviation security in Canada. In doing so, it should adopt a national risk management protocol based on best practices and using a performance standard of continuous improvement, delivering levels of risk in all relevant areas that are as low as reasonably achievable. Where acceptable levels have not been achieved, resources must be allocated on a priority basis to address the risk appropriately.
- 6.1. To facilitate clear communication and understanding, Transport Canada should require those responsible for aviation security to follow a common set of risk management protocols consistent with the national protocol. Transport Canada should require all stakeholders to:
 - a. Provide a detailed description, in their respective security programs that are submitted to Transport Canada for acceptance or approval, of the risk management protocol employed for their operations;
 - b. Systematically employ these risk management protocols in the development and implementation of aviation security measures, policies, practices and procedures for their operations; and
 - c. Promote coordinated risk management decision-making by engaging in ongoing dialogue with Transport Canada and other stakeholders through participation in AGAS and its technical

committees, and elsewhere as necessary, to ensure clarity, precision and a shared understanding of terminology and methodologies.

- 6.2. Each year, the Minister of Transport should certify that the civil aviation security regime in Canada possesses:
 - a. A common set of protocols for carrying out risk management, based on current best practices;
 - b. A performance standard of continuous improvement, delivering levels of risk in all relevant areas that are as low as reasonably achievable; and
 - c. Acceptable levels of risk control in all domains of risk.
- 6.3. Periodic assessment of Transport Canada's risk management protocol by the Auditor General is encouraged.

Recommendation 7

7. There should be no significant gaps in civil aviation security. When a significant deficiency is identified, the best interim measures must be implemented to address the risk while more permanent measures, including technological solutions, are developed.
 - 7.1. The civil aviation security regime must be capable of redeploying resources so that all significant threats are adequately addressed and measures do not disproportionately emphasize a particular threat, such as the threat posed by passengers and baggage.
 - 7.2. As soon as improved equipment and measures become available, they should be deployed.
 - 7.3. If, after a systematic risk management process, a decision is made not to implement measures that address a given threat, measures should nonetheless be designed for emergency implementation if the threat subsequently becomes imminent.
 - 7.4. Legislative initiatives to improve civil aviation security should not be subject to unreasonable delay.

Recommendation 8

8. Transport Canada and others responsible for civil aviation security should foster a culture of security awareness and constant vigilance. As part of this endeavour, a comprehensive public education campaign should be developed to increase awareness of the measures in place for the public's protection and the role the public can play in promoting security.

III. Use of Intelligence

Recommendation 9

9. Transport Canada must provide timely, relevant and actionable intelligence information to civil aviation stakeholders, with the primary recipients being airport operators, air carriers, pilots, CATSA, FBOs and GA facilities.
 - 9.1. Transport Canada should be guided by the “need to share” principle and should cooperate more closely with key stakeholders to ensure they receive the intelligence information they require.
 - 9.2. Aviation stakeholders should provide Transport Canada with feedback about the quality and timeliness of intelligence they receive. Where concerns are raised, a collaborative approach to resolving those concerns should be taken.
 - 9.3. In addition to threats related to airports and air carriers, aviation stakeholders should be kept abreast of changes to the general threat environment. Regular security briefings for all stakeholders, including front-line workers, should occur.

IV. Airport Security

Recommendation 10

10. Non-Passenger Screening (NPS) should be improved at all designated airports in Canada on a priority basis.
 - 10.1. Full (100 per cent) NPS should be implemented upon entry to restricted areas at all Class 1 and Class 2 airports, with random NPS upon exit at Class 1 airports.
 - 10.2. NPS upon entry at Class Other and upon exit at Class 2 and Class Other airports should be implemented as necessary, based on risk.

Recommendation 11

11. Perimeter security should be improved at all designated airports on a priority basis.
 - 11.1. Perimeter security should be enhanced with physical and technological barriers and appropriate monitoring, based on risk.

- 11.2. Transport Canada should conduct intrusion tests of airport perimeters.

Recommendation 12

12. All vehicles entering airside and restricted areas at Class 1 airports should be subject to a full search, including full NPS of occupants. Vehicles entering Class 2 airports should be searched as necessary, based on risk.

- 12.1. Where supply chain security measures have been applied to vehicles, a search may be confined to the areas of the vehicle that have not been secured, and should include full NPS of occupants.

CATSA's mandate should be expanded on a priority basis to include searching vehicles and screening their occupants. CATSA should be provided with the necessary funding.

Recommendation 13

13. The Restricted Area Identification Card (RAIC) should be implemented at all 89 designated airports on a priority basis, and should be expanded to include perimeter security, including vehicle gates, FBOs and tenant facilities.

- 13.1. RAICs, Restricted Area Passes (RAPs) and temporary or visitor passes should be worn and clearly displayed at all times by all individuals who access restricted and airside areas of the airport.

- 13.2. All access control devices, including RAICs and RAPs, should be implemented in a manner that prevents "piggybacking," "tailgating" and other means of gaining unauthorized access.

- 13.3. All RAICs and RAPs, as well as employee uniforms and any other form of airport identification belonging to former airport employees, should be diligently accounted for, retrieved and/or deactivated. Appropriate penalties should be imposed for failing to return such items.

Recommendation 14

14. For FBOs and GA facilities attached to designated airports, access to the airports' airside and restricted areas should be strictly controlled through RAICs, full NPS and vehicle searches.

Recommendation 15

15. Transport Canada should improve its policies and procedures governing transportation security clearances.

- 15.1. Transport Canada and the RCMP should increase efforts to share information on individuals applying for a transportation security clearance to work at airports.
- 15.2. Transport Canada should establish a formal process, including specific criteria, for reviewing applications for security clearances made by individuals with a criminal record.
- 15.3. Transport Canada should reinstate credit checks as a component of the security clearance process before issuing an RAIC for non-passengers who require access to restricted areas at airports.
- 15.4. Transport Canada should take steps to reduce the delay in processing applications for transportation security clearances.

Recommendation 16

- 16. Security measures should be developed and implemented to protect public areas of air terminal buildings at Class 1 airports, based on risk.

Recommendation 17

- 17. All airports should develop and implement a security awareness and constant vigilance program that includes training for all airport workers employed in air terminal buildings and airside portions of airports.

V. Passenger and Baggage Screening

Recommendation 18

- 18. Current methods for conducting pre-board screening (PBS) are comprehensive, but improvements are required in their application.
- 18.1. Although technology has enhanced the ability to effectively conduct PBS, that technology should rarely be relied upon exclusively.

When selecting equipment and procedures for passenger screening, consideration should be given to individual rights, including privacy rights and the rights guaranteed under the *Canadian Charter of Rights and Freedoms*. In particular, any consideration of behavioural analysis techniques as a tool for PBS must include a thorough review. Concerns about the risk of racial, ethnic and religious profiling must be given specific and careful attention. If a decision is made to implement such a program, the following must be addressed: effectiveness of the measure; competencies, training (initial and ongoing) and testing required of those who would conduct the analysis; and oversight requirements.

- 18.2. Given the importance of the “no search, no fly” rule and the potential impact of security measures on individual rights, Transport Canada and the Office of the Privacy Commissioner of Canada should collaborate to devise tools and criteria to evaluate proposed security measures.

Recommendation 19

19. Although the multi-level system in place for Hold Bag Screening (HBS) is comprehensive, some improvements are required.
 - 19.1. Baggage should never be loaded onto an aircraft without a passenger-baggage reconciliation. Interlined baggage, in particular, must be subjected to comprehensive passenger-baggage reconciliation prior to being loaded.
 - 19.2. Consideration should be given to whether the current administrative monetary penalties for non-compliance with passenger-baggage reconciliation procedures provide sufficient deterrence and reflect the gravity of the potential consequences of non-compliance.
 - 19.3. Although technology has enhanced the ability to effectively screen checked baggage, that technology should rarely be relied upon exclusively.

VI. Use of Technology and Explosives Detection Dogs

Recommendation 20

20. Transport Canada should ensure that all screening technology is reliable and effective. This requires assessment not only during the development and deployment stages, but also continual assessment during conditions of actual use.
 - 20.1. Transport Canada should ensure that screening officers operating equipment are adequately trained and regularly tested to ensure their competence.
 - 20.2. Transport Canada should ensure that screening equipment is properly maintained.

Recommendation 21

21. The use of explosives detection dogs should be evaluated and expanded as appropriate. Consideration should be given to their use in:

- a. PBS and HBS;
- b. Screening of air cargo; and
- c. Perimeter security, including the screening of vehicles.

VII. Screeners

Recommendation 22

22. CATSA should find long-lasting solutions to resolve difficulties in the recruitment of appropriately qualified screening contractors and in the recruitment, retention, training and oversight of competent screening officers to ensure the highest quality of screening.
- 22.1. Because of the voluminous material that all screening officers are required to master, consideration should be given to specifying a minimum educational requirement for them in the *Designation Standards for Screening Officers*.
 - 22.2. Given the importance of their work, screening officers should receive appropriate compensation and employee benefits to reduce difficulties in retaining them.
 - 22.3. Because of the challenges associated with their duties, particularly repetitive, stressful and monotonous work that only rarely results in finding prohibited items, CATSA should make ongoing efforts to instill greater sense of mission and morale among screening officers:
 - a. Consideration should be given to creating an employment structure that provides opportunities for advancement; and
 - b. Consideration should be given to holding regular briefings for screening officers, particularly at Class 1 airports, to provide relevant intelligence updates, as well as information relating to prohibited items, methods of concealment and information contained in recent Transport Canada bulletins.
 - 22.4. Screening officer duties should focus solely on preventing unlawful interference with civil aviation. Screening officers should not be mandated to search for contraband or other items that may interest law enforcement, but that are not relevant to CATSA's mandate.

- 22.5. Given the changing nature of threats to aviation, training of screening officers should be continuous. Training should include instruction in practical skills and in the detection of improvised explosive devices (IEDs).
- 22.6. Training of screening officers should be designed to foster a general culture of security awareness and constant vigilance.
- 22.7. CATSA should continue to use training and motivational tools such as X-ray Tutor (XRT) and the Threat Image Projection System (TIPS).
- 22.8. Where screening officer deficiencies are identified, immediate steps, primarily additional training, should be taken to ensure competence.
- 22.9. Transport Canada should define clear and consistent system-wide performance standards for CATSA, in addition to the failure rate for infiltration tests, against which compliance and effectiveness can be assessed. Performance measures should define whether CATSA's performance is satisfactory or unsatisfactory:
 - a. This should include agreement between Transport Canada and CATSA regarding the threshold for failure of infiltration tests and the specific elements that constitute failure; and
 - b. CATSA's response to failed infiltration tests should emphasize re-training, and should include documentation of corrective action taken and timely written responses to Transport Canada enforcement letters and related enquiries.
- 22.10. Whenever the Auditor General of Canada deems it necessary, the Auditor General should review the changes implemented by CATSA to address problems with recruitment, retention, training, testing and oversight of screening officers.

VIII. Air Cargo and Other Non-Passenger Items

Recommendation 23

23. A comprehensive system for screening air cargo (including mail) for transport on passenger and all-cargo aircraft should be implemented as an urgent priority. Canada's system of Known Shippers should be discontinued as soon as possible, and a system of Regulated Agents put in its place in accordance with international best practices. In designing and implementing the system, the Government should exceed the minimum requirements of Annex 17 of the *Chicago Convention*, with the aim of achieving the highest possible standards of air cargo security.

- 23.1. The Commission supports Transport Canada's proposed Air Cargo Security (ACS) Initiative and recommends its implementation on a priority basis.
- 23.2. Under the new regime, all air cargo to be loaded onto passenger aircraft should be screened to a level comparable to that currently provided for hold baggage.
- 23.3. All air cargo to be loaded onto all-cargo aircraft should be screened to a level deemed appropriate, on the basis of risk. When air cargo is transferred from all-cargo to passenger aircraft, additional screening should be conducted commensurate with screening requirements that normally apply to air cargo carried on passenger aircraft.
- 23.4. Screening for air cargo should take into account the risk posed by new, emerging or otherwise unaddressed threats as they arise.
- 23.5. The evaluation of technologies to screen consolidated or bulk cargo should be accelerated.
- 23.6. A centralized screening service for all air cargo requiring screening at the airport should be considered for all Class 1 airports.
- 23.7. CATSA, with its screening mandate, expertise, equipment and dedicated personnel, is the appropriate authority to conduct air cargo screening services at the airport and may have a role to play in the oversight and inspection of screening by Regulated Agents. CATSA's mandate should be expanded by legislation to include the screening of air cargo.
- 23.8. Care must be taken to provide adequate training for all air cargo screeners. This should include rigorous testing for required competencies. The development and implementation of computer software training and screening aids should be accelerated.
- 23.9. Transport Canada should employ a sufficient number of security inspectors trained and qualified for inspecting, testing, auditing and enforcing the new air cargo security regime.
- 23.10. Funding for the ACS Initiative must ensure that it remains sustainable and can respond to emerging or otherwise unaddressed threats.
- 23.11. Annual progress reports on enhancements in air cargo security should be provided to Parliament by the Minister of Transport for each of the five years following release of the Commission's report.

Recommendation 24

24. The new security regime for air cargo must be governed by legislation, not by non-binding Memoranda of Understanding. The security regime should reflect international best practices.

24.1. Legislative provisions should include, but not be limited to, the following:

- a. Mandatory security programs for all Regulated Agents, with formal approval from Transport Canada;
- b. Clear definitions for terminology, including the terms “screen,” “inspect” and “search”;
- c. Measures and technologies for screening air cargo;
- d. Screening requirements for all Regulated Agents, whether shippers, freight forwarders or air carriers;
- e. Appropriate training requirements for all Regulated Agents, their employees and sub-contractors;
- f. Requirements to maintain the security of off-airport premises to a specified level wherever cargo is handled, stored and potentially accessed;
- g. Requirements to maintain the security of off-airport vehicles to a specified level for the transport of air cargo to its final point of transfer;
- h. Requirements for ensuring appropriate access and security controls for air cargo while on airport premises, during transfer to the aircraft and on loading onto the aircraft;
- i. Mandatory security clearances, including a credit check, for all workers who have access or potential access to air cargo from the point of receipt to the point of transfer, including sub-contractors engaged to handle cargo on behalf of a Regulated Agent;
- j. A system of inspection, testing, auditing and enforcement by Transport Canada or its designated agent; and
- k. Methods of enforcement, including administrative monetary penalties and other penalties that reflect the potential gravity of the consequences of non-compliance.

- 24.2. Regulated Agent security programs should describe all measures, practices, policies and procedures applicable to air cargo security that have been, or will be, implemented by the Regulated Agent, including security awareness programs and risk management protocols.

Recommendation 25

25. A supply chain security regime should be established for other non-passenger items (such as stores and catering) that are prepared at off-airport premises before being delivered to an aircraft.

IX. Fixed Base Operations and General Aviation

Recommendation 26

26. As an urgent priority, all passengers and carry-on and checked baggage boarding flights at FBOs and GA facilities that feed into designated airports or are attached to designated airports should be screened to a level comparable to passenger and baggage screening for scheduled commercial flights.
 - 26.1. As an equally urgent priority, all non-passengers entering such FBO and GA facilities should be screened to an acceptable level, based on appropriate risk management protocols;
 - 26.2. All non-passenger items (including air cargo) to be placed on flights departing from such FBO and GA facilities should be screened to an acceptable level, based on appropriate risk management protocols.
 - 26.3. On a priority basis, all FBO and GA facilities should develop and implement a security awareness and constant vigilance program that supports a “neighbourhood watch” approach to security. An accompanying training program should be developed and implemented for all personnel to foster a culture of security awareness and constant vigilance.
 - 26.4. CATSA should oversee security screening services at FBOs and GA facilities. If CATSA’s resources are engaged, additional government funding should be provided.
 - 26.5. The aviation security requirements for FBOs and GA facilities should be governed by legislation.

XI. Duty to Warn and Transparency

Recommendation 27

27. The development of a public warning system for threats against airlines should receive further study. Issues include:
- a. international experience with such systems;
 - b. the circumstances under which public warnings of threats have occurred in Canada;
 - c. the proper balance between security and industry interests;
 - d. the proper balance between the need for secrecy and the need to instill public confidence;
 - e. the appropriate threshold at which a public warning should be issued; and
 - f. the policy and legal implications, including possible liability to air carriers whose operations could be compromised by a public warning.

Recommendation 28

28. In general, greater transparency in aviation security is required to inspire confidence in the system, to provide assurance that resources are effectively allocated and to ensure that government and industry stakeholders remain accountable for managing this mandate.
- 28.1. The Commission does not recommend publishing intrusion test results. If a decision is nonetheless made to publish them, publication should only occur after enough time has passed to enable vulnerabilities identified by the tests to be addressed.

XII. Funding

Recommendation 29

29. As a core mandate directly related to national security, civil aviation security should receive sustained funding, regardless of prevailing economic circumstances, to maintain an acceptable level of security.

- 29.1. Funding for civil aviation security should be derived primarily from government.
- 29.2. Funding priorities should be directed to areas of risk that have not achieved an acceptable level of risk control, such as air cargo and control of access to airside and restricted areas of airports.
- 29.3. If additional funds are required for initiatives related to passenger and baggage security, the Commission supports the continuance of an Air Travellers Security Charge (ATSC). However:
 - a. The collection, retention and disbursement of the ATSC should be subjected to comprehensive and transparent accounting. All revenue from the ATSC should be traceable and should be used solely for civil aviation security;
 - b. An annual report of ATSC revenues as well as expenditures by program or department is recommended; and
 - c. CATSA should be the main beneficiary of funds from the ATSC.

APPENDIX A

Chronology:

Significant Acts of Unlawful Interference with Civil Aviation

1931

February 21, 1931

First recorded incident of air terrorism against commercial aviation. A Pan American Airways mail aircraft was hijacked in Peru. The aircraft was commandeered by a group of Peruvian revolutionaries with the intention of dropping propaganda leaflets. There were no casualties.¹

1933

October 10, 1933

First proven case of sabotage in the history of commercial aviation. A United Airlines Boeing 247 crashed while en route from Cleveland, Ohio to Chicago, Illinois. The aircraft was destroyed by an explosive device using nitroglycerine, likely attached to a timing device. The bomb was thought to have been placed on board, possibly concealed in a brown package. All 7 on board were killed.²

1948

April 6, 1948

First case of air piracy related to escape from the Iron Curtain. A CSA flight was hijacked from Prague to Bratislava, Czechoslovakia. The aircraft was seized by roughly three-quarters of the 26 persons on board and landed safely in an American zone of Germany, near Munich.³

1949

September 9, 1949

Near Sault Au Cochon, Quebec, a bomb exploded in a forward baggage compartment of a Quebec Airways (Canadian Pacific) DC-3, killing 23 people. Albert Guay and two accomplices (the bomb maker and the person who delivered the package containing the bomb to the plane) were tried, convicted and executed.⁴ Guay's wife had been insured, with Guay as the beneficiary. Aircraft bombings to support insurance scams with murder or suicide as the means was to become a feature of aviation sabotage in the 1950s and 1960s.

¹ Exhibit P-448, p. 10.

² Exhibit P-448, p. 10.

³ Exhibit P-448, p. 10.

⁴ Exhibit P-35, p. 36; Exhibit P-147, p. 14.

1950

April 13, 1950

An explosive device detonated in the lavatory of a British European Airways aircraft flying from London, UK, to Paris. Of the 32 persons on board, 1 crew member was seriously injured. The aircraft landed safely.⁵

1952

September 24, 1952

A bomb placed in a suitcase exploded aboard a flight from Mexico City to Oaxaca de Juarez, Mexico. Two passengers suffered injuries.⁶

1955

April 11, 1955

An Air India International Lockheed 749A, originating at Hong Kong, was carrying Chinese delegates and journalists on their way to a conference in Bandung, Indonesia. A bomb exploded while the aircraft flew over the South China Sea. A Chinese aircraft cleaner had reportedly been bribed to place an incendiary device in the starboard wheel well, an early example of an airport worker being used to aid in the sabotage of an aircraft. Only 3 of the 19 persons on board survived. Political terrorism was the apparent motive behind the sabotage of this aircraft.⁷ It is thought that Chinese Premier Zhou Enlai was the target of this act of sabotage. His travel plans had been kept secret and he left China three days later.⁸

November 1, 1955⁹

A United Airlines flight exploded over Longmont, Colorado. All 44 on board were killed. A bomb had been placed on board by a saboteur, who had purchased life insurance on his mother, a passenger on the flight. He was reportedly inspired by the 1949 Albert Guay Affair in Quebec.¹⁰

⁵ Exhibit P-448, p. 13.
⁶ Exhibit P-448, p. 14.
⁷ Exhibit P-448, p. 15.
⁸ Exhibit P-447, p. 1.
⁹ Exhibit P-447, p. 2.
¹⁰ Exhibit P-448, pp. 94-95.

1956

March 4 and April 27, 1956 A Greek Cypriot EOKA bombing campaign against British rule in Cyprus led to the destruction of a British aircraft¹¹ by an explosive device in a cargo compartment while it was parked at Nicosia airport on March 4, 1956. A Dakota was destroyed on April 27, 1956.¹²

1959

A Pan Am flight was hijacked during a coup in Peru.¹³

A Cuban internal flight was hijacked by Raúl Castro in 1959 as the first political hijacking.¹⁴

November 1, 1958 A Cuban airliner was hijacked by the Twenty-Sixth of July Movement and forced to attempt a night landing in a remote airfield in Cuba. The aircraft crashed, killing 17 of the 20 people on board.¹⁵

September 8, 1959 A bomb in a suitcase was suspected in the mid-air explosion of a Douglas DC-3 in Mexico. The aircraft landed safely. The saboteur was the only person killed when he was ejected from the aircraft during the explosion. Seven others suffered injuries.¹⁶

1960

January 6, 1960 An explosion occurred in the passenger cabin of a National Airlines aircraft while in flight. The blast beneath a seat caused the DC-6B to crash into the ground in North Carolina. All 34 persons aboard were killed. A suicide-for-insurance scheme was suspected.¹⁷

¹¹ Exhibit P-35, p. 36.

¹² Exhibit P-35, p. 36.

¹³ Exhibit P-35, p. 36.

¹⁴ Exhibit P-35, p. 36.

¹⁵ Exhibit P-35, p. 36.

¹⁶ Exhibit P-448, p. 17.

¹⁷ Exhibit P-448, pp. 96-98.

1961

May 1, 1961¹⁸

First ever successful hijacking of a domestic carrier in the United States. The aircraft was forced to fly to Communist Cuba. Puerto Rican born Abntulio Ramirez Ortiz¹⁹ forced the National Airlines Convair 440²⁰ to fly to Havana at gun point, where he was given asylum. He was imprisoned for twenty years when he returned to the United States in 1975.²¹

May 10, 1961

An Air France aircraft crashed in the Sahara Desert, killing all 78 persons aboard. The airline concluded that the most probable cause was sabotage with a nitrocellulose explosive.²²

1962

May 22, 1962

First successful sabotage of a commercial jet airliner. A Continental Air Lines Boeing 707 crashed along the Iowa/Missouri border in the United States, killing all 45 persons aboard. Dynamite had been detonated in the used towel bin in the lavatory.²³

1965

A grenade was thrown at the Aden airport terminal in Yemen, injuring 7 British children.²⁴

1966

November 22, 1966²⁶

El Condor nationalists hijacked an Argentinean aircraft from Buenos Aires to the British-ruled Falkland Islands in a bid to bring attention to Argentina's claim to the islands. They eventually surrendered their hostages and were returned to Argentina by British authorities.²⁵

An Aden Airways Douglas DC-3 aircraft was blown up in mid-air near Aden, Yemen, killing all 30 persons on board. The bomb had been placed in hand baggage carried into the cabin.²⁷

18 Exhibit P-448, p. 18.
 19 Exhibit P-35, p. 36.
 20 Exhibit P-448, p. 18.
 21 Exhibit P-35, p. 36.
 22 Exhibit P-448, pp. 18-19.
 23 Exhibit P-448, p. 98.
 24 Exhibit P-35, p. 36.
 25 Exhibit P-35, p. 36.
 26 Exhibit P-448, p. 170.
 27 Exhibit P-448, p. 21.

1967	
June 30, 1967	An aircraft carrying Katangan rebel leader Moise Tshombe was hijacked en route to Ibiza, Spain, and forced to land in Algeria in a bid to extradite him to his native Congo. Algeria kept him under house arrest until he died two years later. ²⁸
October 12, 1967 ²⁹	A British European Airways Comet aircraft was destroyed by a bomb, detonated in the passenger cabin, while it flew over the Mediterranean Sea. All 66 persons on board were killed. ³⁰
1968	
February 21, 1968	A Delta Airlines DC-8 was forced to fly to Havana, Cuba, in the first successful hijacking of a US commercial airliner since 1961. The hijacker was granted political asylum. ³¹ This hijacking to Cuba was followed by a number of such incidents in 1968 involving American and other countries' aircraft. In addition, there were failed attempts to take seized aircraft to Cuba. Hijackings to Cuba continued throughout the next two decades. ³²
July 23, 1968	Popular Front for the Liberation of Palestine supporters seized an El Al Boeing 707 in Rome, Italy, and diverted it to Algeria, where 32 Jewish passengers were held hostage for five weeks. ³³ This was the first hijacking of a commercial flight in or out of the Middle East. ³⁴

²⁸ Exhibit P-35, p. 37.

²⁹ Exhibit P-448, p. 119.

³⁰ Exhibit P-448, p. 119.

³¹ Exhibit P-35, p. 37.

³² For example: 12 March – National; 21 March – Avensa (Venezuela); 19 June – Viasa (Venezuela); 29 June – Southeast; 1 July – Northwest; 17 July – National; 20 September – Eastern; 22 September – Avianca (Colombia); 6 October – Aeromaya (Mexico); 4 November – National; 18 November – Mexicana (Mexico); 23 November – Eastern; 24 November – Eastern; 30 November – Eastern; 11 December – TWA; 19 December – Eastern. See Exhibit P-448, pp. 23-25.

³³ Exhibit P-35, p. 37; see also Exhibit P-263, Tab 4.

³⁴ Exhibit P-448, p. 67.

December 26, 1968

An Israeli was killed in a Popular Front for the Liberation of Palestine machine gun attack on an El Al aircraft at Athens airport, Greece. Two terrorists were captured but later released by the Greek government after a Greek aircraft was hijacked to Beirut. Three days after the Athens attack, Israeli commandos raided Beirut airport in Lebanon and blew up 13 Arab airliners in retaliation.³⁵

1969

February 18, 1969

Palestinian terrorists attacked an El Al Boeing 707 on the runway at Zurich Airport in Switzerland, raking the fuselage with gunfire and killing the pilot and 3 passengers. An Israeli sky marshal/security guard returned fire, killing one of the terrorists.³⁶

August 29, 1969

A Trans World Airlines (TWA) aircraft was hijacked by the Popular Front for the Liberation of Palestine terrorists after taking off from Rome, Italy. It was forced to fly to Damascus, Syria. All of the passengers and crew were released unharmed, but the terrorists detonated a bomb in the cockpit of the aircraft.³⁷ The hijackers were led by Leila Khaled who was to lead the group responsible for the Dawson's Field incident in 1970.

December 22, 1969

An Air Vietnam Douglas DC-6B, on a scheduled domestic flight over South Vietnam, from Saigon to Da Nang, sustained substantial damage when an explosive device detonated in its cabin as it descended to land at Nha Trang, an en-route stop. Most of the 34 persons killed were on the ground. Among the 77 persons on board the aircraft, all but 10 passengers survived. The bomb had exploded near the front left lavatory.³⁸

³⁵ Exhibit P-35, p. 37. See also Exhibit P-448, p. 67

³⁶ Exhibit P-35, p. 37.

³⁷ Exhibit P-35, p. 37.

³⁸ Exhibit P-448, pp. 121-122.

1970

February 10, 1970

Three Arab terrorists attempted to hijack an El Al Boeing 707 at Munich airport, Germany, but were thwarted by the pilot who grappled with a terrorist in the terminal lounge. One Israeli was killed and 11 others were wounded.³⁹

February 21, 1970

Shortly after take-off, a Swissair aircraft reported a suspected explosion in the aft compartment. The aircraft crashed into a forest, killing all 47 persons on board. The bombing was suspected to be the work of Arab terrorists.⁴⁰

September 6, 1970⁴¹

The first coordinated multiple hijacking resulted in the events that took place at Dawson's Field, Jordan. TWA, Swissair and, three days later, a BOAC aircraft, along with more than 300 hostages, were hijacked and flown to an abandoned RAF field in the Jordanian desert⁴² by the members of the Popular Front for the Liberation of Palestine. The BOAC VC-10 was seized following the capture of the ringleader, Leila Khaled, during a failed attempt to hijack an El Al aircraft, a target of the original plan. The BOAC hijacking was used as a bargaining chip to free Khaled, who was being held in London. Two other members of the PFLP terrorist group, who had failed to board the EL Al aircraft in Amsterdam, seized a Pan Am 747 as a target of opportunity and flew it to Cairo where it was destroyed after the passengers were released. The German, Swiss and British Governments all agreed to the PFLP's demands and released a number of terrorists held in their jails, including Leila Khaled.⁴³ This incident is generally considered to represent the birth of modern air terrorism.⁴⁴

³⁹ Exhibit P-35, p. 37

⁴⁰ Exhibit P-448, pp. 68-69.

⁴¹ Exhibit P-448 reports the relevant dates as September 6-12, 1970; see p. 70.

⁴² Testimony of Rodney Wallis, vol. 35, May 29, 2007, pp. 4207-4208.

⁴³ Exhibit P-35, p. 37.

⁴⁴ Exhibit P-259: Rodney Wallis, *Combating Air Terrorism* (New York: Brassey's, 1993), p. 92 [Wallis, *Combating Air Terrorism*].

1971

November 12-13,
1971

A terrorist claiming to be a member of the Irish Republican Army hijacked Air Canada Flight 812, which was en route from Vancouver to Toronto. The hijacker took over the aircraft with a sawed-off shotgun and was allegedly armed with dynamite. The aircraft landed twice in Grand Falls, Montana, first for fuel and money, and the second time to release all the passengers.⁴⁵

December 26, 1971⁴⁶

Patrick Critton, a member of the black liberation group, Republic of New Africa,⁴⁷ hijacked Air Canada Flight 932 from Thunder Bay to Toronto, Ontario. He allegedly brandished a handgun and a grenade and demanded to be flown to Cuba.⁴⁸

1972

March 7-8, 1972

In an extortion plot, Trans World Airlines was informed that bombs had been placed on four of its aircraft. One bomb was discovered aboard Flight 7, a domestic transcontinental service from New York City to Los Angeles. On March 8, another bomb exploded in the cockpit of a Boeing 707 while it was on the ground in Las Vegas, Nevada. There were no injuries. Although the perpetrators demanded \$2 million, no money was collected, nor were any suspects apprehended.⁴⁹

May 9, 1972

A Belgian Sabena aircraft was hijacked en route from Vienna and forced to land at Ben Gurion Airport in Tel Aviv, Israel, where Israeli commandos stormed the aircraft.⁵⁰ Four Palestinian Black September terrorists on board the aircraft were killed and the hostages were freed. One passenger and 5 Israeli soldiers were killed.⁵¹

⁴⁵ Exhibit P-448, p. 100.

⁴⁶ Exhibit P-488, p. 37.

⁴⁷ Exhibit P-147, p. 10.

⁴⁸ Exhibit P-35, p. 38.

⁴⁹ Exhibit P-448, p. 128.

⁵⁰ Exhibit P-147, p. 11.

⁵¹ Exhibit P-35, p. 38.

August 16, 1972	An explosive device hidden in a record player detonated in the aft baggage compartment of an El Al Boeing 707 jetliner shortly after it left Rome, Italy, bound for Tel Aviv, Israel. The aircraft landed safely. There were no serious injuries among the 153 persons aboard the aircraft. ⁵²
May 30, 1972	The “Lod Airport Massacre” took place when the Popular Front for the Liberation of Palestine and Japanese Red Army terrorists opened fire in the passenger terminal of Lod (re-named Ben Gurion) Airport in Israel. Twenty-six civilians were killed and 78 were wounded. ⁵³
October 29, 1972	Four hijackers, wanted for murdering a bank manager and a policeman during a failed bank robbery, killed a ticket agent and wounded a ramp serviceman while forcing their way aboard an Eastern Air Lines Boeing 727. They demanded to be taken to Cuba. ⁵⁴
November 10, 1972	The longest and perhaps most grueling of the Cuban hijackings involved Southern Airways Flight 49. The DC-9 was hijacked by three fugitives in the United States, landing in several locations in the US, as well as in Toronto, before finally landing in Havana, Cuba. The incident lasted 30 hours. At one point, the aircraft circled the country retreat of the American President, Richard Nixon, and at another, the hijackers threatened to crash the aircraft into the atomic power plant in Oak Ridge, Tennessee. ⁵⁵
December 8, 1972	A failed attempt by the Eritrean Liberation Front to hijack an Ethiopian Airlines Boeing 720B while in flight from Addis Ababa to Asmara left seven of the hijackers dead, killed by security guards. Two of those killed were women. The aircraft returned safely to Addis Ababa. ⁵⁶

52 Exhibit P-448, p. 74.
 53 Exhibit P-147, p. 22.
 54 Exhibit P-447, p. 3.
 55 Exhibit P-448, p. 38.
 56 Exhibit P-448, p. 56.

1973	
August 5, 1973	A Black September suicide squad attacked the passenger terminals at Athens Airport in Greece, killing 3 civilians and injuring 55.
November 17, 1973	Palestinian terrorists bombed a Pan Am office at Fiumicino Airport in Rome, killing 32 and injuring 50. The terrorists then took 7 Italian policemen hostage and hijacked an aircraft to Athens, Greece. After killing one hostage, they flew to Kuwait. The terrorists eventually surrendered. ⁵⁷
1974	
August 26, 1974	A bomb malfunctioned and a fire was discovered in the aft baggage compartment of TWA Flight 841, a Boeing 707, after the aircraft had landed in Rome on a flight from Athens. There were no injuries, but Flight 841 was again targeted by terrorists just two weeks later. ⁵⁸
September 8, 1974 ⁵⁹	A bomb exploded in the baggage compartment ⁶⁰ of TWA Flight 841 while it flew over the Ionian Sea off the coast of Greece. All 88 persons aboard, including 79 passengers and 9 crew members, were killed. ⁶¹ The attack was the work of the Popular Front for the Liberation of Palestine. ⁶² The bomb had been placed on board at Athens, which had been known for its lax security. Subsequently, TWA instituted a policy of inspecting all baggage placed on board its aircraft. ⁶³
November 23, 1974	A British DC-10 aircraft was hijacked by Palestinian Rejectionist Front terrorists at Dubai in the United Arab Emirates. The aircraft was flown to Tunisia where a German passenger was killed. ⁶⁴

⁵⁷ Exhibit P-35, p. 38; see also Exhibit P-263, Tab 4.
⁵⁸ Exhibit P-448, p. 76.
⁵⁹ Exhibit P-448, p. 76.
⁶⁰ Exhibit P-35, p. 38.
⁶¹ Exhibit P-448, p. 76.
⁶² Exhibit P-35, p. 38.
⁶³ Exhibit P-448, pp. 75-76.
⁶⁴ Exhibit P-263, Tab 4.

1975

January 13, 1975

A missile fired at an El Al Israel Airlines Boeing 707 jet struck a parked DC-9 at Orly Airport in Paris, leaving a hole in its fuselage. Three persons suffered minor injuries, including a crew member. There were no casualties among the 148 persons aboard the 707.⁶⁵

Arab terrorists attacked Orly Airport in Paris, France, seizing 10 hostages in a terminal bathroom. The French government eventually provided the terrorists with a plane to fly them to Baghdad, Iraq.⁶⁶

December 29, 1975

A bomb was detonated at LaGuardia Airport, New York. Eleven people died and 74 were injured.

1976

June 27, 1976

An Air France aircraft was hijacked by a joint German Baader-Meinhof/Popular Front for the Liberation of Palestine terrorist group, and its crew were forced to fly to Entebbe Airport in Uganda. The 258 passengers and crew were held hostage, but all non-Israeli passengers were eventually released. On 3 July, Israeli commandos flew to Uganda and rescued the remaining hostages. All of the terrorists were killed in the rescue, as were 3 passengers, 1 commando and at least 20 Ugandan soldiers.⁶⁷

August 11, 1976

Popular Front for the Liberation of Palestine and Japanese Red Army terrorists attacked a passenger terminal at Istanbul airport in Turkey, killing 4 civilians and injuring 20.⁶⁸

⁶⁵ Exhibit P-448, p. 77.

⁶⁶ Exhibit P-35, p. 38; see also Exhibit P-263, Tab 4.

⁶⁷ Exhibit P-35, p. 38; see also Exhibit P-448, p. 77.

⁶⁸ Exhibit P-35, p. 38.

September 10, 1976

A TWA aircraft en route from New York to Paris was hijacked by Croatian terrorists, who seized 93 hostages. The terrorists surrendered in Paris and released the hostages.⁶⁹

October 6, 1976

Cubana Airlines Flight 455 crashed off the coast of Barbados, killing all 73 people aboard, following the detonation of explosives left by passengers who had exited the plane in Barbados, a transit stop. The attack was blamed on anti-Castro Cuban exiles.⁷⁰ A decade later, two men were sentenced to 20 years' imprisonment for their involvement in the crash.⁷¹

1977

October 13, 1977⁷²

Four Palestinian terrorists hijacked a German Lufthansa Boeing 737 and ordered it to fly around a number of Middle East destinations for four days. After the terrorists killed the plane's pilot, the aircraft was stormed by German counter-terrorist troops, assisted by two British Army Special Air Service soldiers, when it landed at Mogadishu in Somalia. All 90 hostages were rescued, and the 3 terrorists were killed.⁷³

1978

February 19, 1978

An aircraft was hijacked at Larnaca Airport in Cyprus by Arab terrorists. After being refused permission to land at a number of Arab capitals, the hijackers returned to Larnaca. Egyptian commandos landed and, without Cypriot government authorization, tried to attack the plane, resulting in a gun battle with Cypriot troops. Fifteen Egyptian troops, 7 Cypriot soldiers and a German cameraman were killed.⁷⁴

August 20, 1978

An El Al stewardess was killed when a crew bus was ambushed by the Popular Front for the Liberation of Palestine terrorists outside the Europa Hotel in London, UK.⁷⁵

⁶⁹ Exhibit p-35, p. 38.

⁷⁰ Testimony of Moses Aléman, vol. 36, May 30, 2007, p. 4266.

⁷¹ Exhibit P-448, p. 136.

⁷² Exhibit P-447, p. 4.

⁷³ Exhibit P-263, Tab 4.

⁷⁴ Exhibit P-35, p. 39.

⁷⁵ Exhibit P-263, Tab 4.

November 15, 1978

Twelve people were injured in a bomb explosion on an American Airlines flight in the United States. The so-called Unabomber is held responsible for the incident.⁷⁶

An Air Florida flight from Key West to Miami in the United States was hijacked by 7 Cubans and flown to Cuba, where they released their hostages and were taken into custody. Six further US aircraft were hijacked to Cuba over the next month. All the passengers were released unharmed.⁷⁷

Three passengers were killed when Cubans hijacked an aircraft in Peru and demanded to be flown to the United States.⁷⁸

The president of United Airlines was injured in a bomb attack in Chicago, that was blamed on the Unabomber.⁷⁹

Four Iranian terrorists were killed when Turkish security forces stormed a hijacked Turkish Airlines aircraft after it landed in eastern Turkey. The terrorists killed 1 of the 155 hostages.⁸⁰

1979

August 27, 1979

A bomb shattered a Turkish airlines office in Frankfurt, Germany, injuring 1 person. The attack was later claimed by the Armenian Secret Army for the Liberation of Armenia (ASALA).⁸¹

76 Exhibit P-35, p. 39.
77 Exhibit P-35, p. 39.
78 Exhibit P-35, p. 39.
79 Exhibit P-35, p. 39.
80 Exhibit P-35, p. 39; see also Exhibit P-147, p. 14.
81 Exhibit P-263, Tab 4.

1980	
June 27, 1980	A twin-jet Douglas DC-9 was destroyed over the Tyrrhenian Sea. All 81 persons aboard were killed. An explosive device, most likely placed between the outer wall of the lavatory and the skin of the aircraft, was determined to be the cause of the crash. No claim of responsibility was ever made, but the incident may have been related to a wave of terrorism blamed on right-wing extremists in Italy. ⁸²
December 21, 1980	An aircraft crashed shortly after take-off in Colombia. All 70 persons on board were killed. An explosive substance, apparently nitroglycerine, had detonated in a rear lavatory. ⁸³
1982	
February 20, 1982	An explosive device hidden in a suitcase detonated on a conveyor belt at the international airport in Managua, Nicaragua. The suitcase had been unloaded from a Boeing 737 jetliner. ⁸⁴
August 11, 1982	An explosive device detonated under a seat in the rear cabin of a Pan American World Airways Boeing 747 flying over the Pacific Ocean. Of the 285 persons aboard, 1 passenger, a 16-year-old boy, was killed in the blast and 15 others suffered injuries. Despite a hole in the cabin floor and a rapid decompression, the aircraft landed safely. The Palestinian responsible for the bombing was captured and prosecuted in Greece. ⁸⁵
1983	
August 19, 1983	A Syrian Arab Airlines 727 jet was severely damaged by an incendiary device while on the ground at Rome, shortly before it was scheduled to depart for Damascus, Syria. All occupants were safely evacuated, with no injuries. ⁸⁶ The improvised explosive device had been placed under a seat in the cabin. This methodology copied that used against Pan Am in August 1982. It was used again in 1985 against TWA.

82 Exhibit P-448, pp. 143-144.
83 Exhibit P-448, p. 145.
84 Exhibit P-448, p. 147.
85 Exhibit P-448, p. 81.
86 Exhibit P-448, pp. 81-82

September 23, 1983

Gulf Air Flight 771, a Boeing Advanced 737, crashed in the desert near Abu Dhabi. All 111 persons on board were killed. Evidence pointed to an act of sabotage. Baggage assigned to the flight had been checked in by a ticket-holder who did not board the aircraft.⁸⁷

1984

December 4, 1984

A Kuwaiti aircraft was hijacked en route to Pakistan from Dubai by Iranian-backed Iraqi Shia terrorists. The aircraft was forced to land in the Iranian capital of Tehran, after two Americans had been killed. The terrorists surrendered to the Iranian authorities and were later released.⁸⁸

January 18, 1984

An explosion in the cargo hold caused major damage to an Air France B-747 over Pakistan. The aircraft landed safely.

1985

April 4, 1985

A rocket was fired into an Alia Jordanian Airlines Boeing 727 that was taking off at Athens, Greece, on a scheduled service to Amman, Jordan. The device failed to explode and the aircraft sustained only minor damage.⁸⁹

Hezbollah terrorists were responsible for a bomb that detonated in the American Airlines offices in Copenhagen.⁹⁰

A Red Army Faction bomb exploded at Frankfurt Airport, Germany, killing 3 people.⁹¹

⁸⁷ Exhibit P-448, p. 82.

⁸⁸ Exhibit P-35, p. 39.

⁸⁹ Exhibit P-448, p. 85.

⁹⁰ Exhibit P-263, Tab 4.

⁹¹ Exhibit P-35, p. 39.

June 14, 1985

TWA Flight 847, a Boeing 727 carrying 8 crew and 145 passengers, was hijacked en route to Rome from Athens by two Lebanese Hezbollah terrorists. The aircraft was forced to fly to Beirut. A two-week hostage ordeal began, in which the aircraft flew twice to Algiers, Algeria. The hijackers demanded the release of prisoners being held in Kuwait as well as the release of 700 Shiite Muslim prisoners held in Israeli and Lebanese prisons. A US Navy diver was killed and 39 passengers were held hostage when demands were not met. The hostages were eventually released after the US Government pressured Israel into releasing hundreds of Lebanese and Palestinian prisoners.⁹²

June 23, 1985

Air India Flight 182, a Boeing 747, was destroyed by a bomb over the Atlantic, killing all 329 people on board. Sikh extremists were blamed for the attack, the worst single air terrorism incident to that time.⁹³ The bomb had been placed in unaccompanied baggage that had been interlined from a CP Air flight to the Air India flight, even though the ticket-holder did not have a reservation on the Air India flight.

June 23, 1985

Two baggage handlers were killed at Narita Airport in Tokyo when a bomb, attributed to Sikh extremists, was placed in an unaccompanied bag that was later offloaded from a CP Air flight arriving from Vancouver to be interlined to Air India Flight 301. The bomb exploded in the transit area.⁹⁴

⁹² Exhibit P-35, p. 40; see also Exhibit P-448, pp. 85-86.

⁹³ Exhibit P-35, p. 40.

⁹⁴ Exhibit P-35, p. 40; see also Exhibit P-147, p. 31.

November 26, 1985

An Egyptair B-727 was hijacked while en route from Athens to Cairo. The aircraft was flown to Malta and shots were exchanged between the hijackers and sky marshals while in flight. On the ground, the terrorists shot 5 passengers, 2 of whom died. An assault by Egyptian Force 777 commandos resulted in the death of some 57 passengers in the ensuing gunfight and when the terrorists set off explosives in the aircraft.⁹⁵

December 27, 1985

Simultaneous suicide grenade and gun attacks by the Abu Nidal terrorist group against passenger terminals at Rome and Vienna airports resulted in 16 persons killed and more than 100 civilians injured.⁹⁶

1986

April 2, 1986

A bomb exploded on a Trans World Airways 727 en route from Rome to Athens. Four passengers, including an infant, were killed when they were ejected from the aircraft at 10,000 feet. It is believed that a bomb was assembled by a female passenger on board using plastic explosives, which she left under her seat. She had boarded the aircraft in Cairo and exited at Athens, but the plane flew on to Rome. The bomb exploded on its return journey.⁹⁷

April 17, 1986

Plastic explosives were placed in hand luggage and were carried unknowingly by an Irish woman, who was to board an El Al Flight in London, UK, bound for Tel Aviv, Israel. The bomb had passed through X-ray security at Heathrow Airport, but was caught by the secondary screening put in place by EL Al. The woman's fiancé had planned the attack. He was subsequently arrested and sentenced to 45 years' imprisonment.⁹⁸

⁹⁵ Exhibit P-35, p. 40.

⁹⁶ Exhibit P-35, p. 40; see also Testimony of Moses Aléman, vol. 35, May 29, 2007, p. 4227.

⁹⁷ Wallis, *Combating Air Terrorism*, pp. 12-13.

⁹⁸ Exhibit P-448, pp. 87- 88.

May 3, 1986	A bomb exploded on an Air Lanka Lockheed 1011 aircraft parked at Colombo Airport, killing more than 20 passengers who were then boarding the aircraft. A customs officer who had access to the aircraft's supplies and who was believed to be sympathetic to the Tamil separatists' movement was arrested and charged with sabotage. The device had been placed in the aircraft's "fly-away" kit, a collection of essential technical items carried on each aircraft to facilitate emergency maintenance at overseas airports. ⁹⁹
August 1986	Rebels fighting the government of the Sudan used a surface-to-air missile (SAM-7) to shoot down an aircraft in flight, killing 60. ¹⁰⁰
September 5, 1986	Terrorists seized a Pan American 747 at Karachi Airport, killing 22 and injuring more than 100. ¹⁰¹ Dressed to resemble airport guards, the terrorists had obtained a vehicle similar to those used by the airport authority. This enabled them free passage through the checkpoint guarding the entrance to the airside. They waved through unchallenged, giving them unimpeded access to the Pan American aircraft, which was being boarded at the time. ¹⁰²
December 25, 1986	An Iraqi 737 was seized and ultimately destroyed following a mid-air gun battle between terrorists and security guards. Grenades were detonated and the gunfight was waged over the bodies of passengers. Seventy-one persons were killed. ¹⁰³
1987	
May 1987	An Air New Zealand aircraft was seized while on the ground at Nandi Airport in Fiji. ¹⁰⁴ The lone would-be hijacker, an employee of a handling company, was persuaded not to carry out the hijacking.

⁹⁹ Wallis, *Combating Air Terrorism*, p. 14.
¹⁰⁰ Wallis, *Combating Air Terrorism*, p. 14.
¹⁰¹ Wallis, *Combating Air Terrorism*, p. 2.
¹⁰² Wallis, *Combating Air Terrorism*, p. 15.
¹⁰³ Wallis, *Combating Air Terrorism*, p. 17.
¹⁰⁴ Wallis, *Combating Air Terrorism*, p. 2.

November 29, 1987

Korean Air Flight 858 was destroyed in flight over the Andaman Sea while en route from Baghdad to Seoul, killing all 115 persons on board. Liquid explosives had been disguised as alcohol and left in an overhead rack by two passengers belonging to the North Korean Workers Party when they disembarked at a transit stop. They had timed the device to detonate on its subsequent sector.¹⁰⁵

December 10, 1987

A US Air service scheduled to operate from Los Angeles to San Francisco was destroyed by a former employee who boarded the aircraft intent on killing his former supervisor who was a passenger. He killed the pilot causing the aircraft to crash. All 43 persons on board died.

1988

March 1, 1988

An explosive device destroyed Commercial Airways (Comair) Flight 206, which was on an internal South African service from Phalaborwa to Johannesburg. The aircraft crashed south-west of Jan Smuts Airport, where it had been scheduled to land. All 17 persons on board were killed. Tests confirmed that the explosive device consisted of nitroglycerine and ammonium nitrate. The person responsible was never identified, but a briefcase known to have been placed aboard at Phalaborwa could not be located. At the time, there were no requirements to screen carry-on baggage at the point of departure. In the wake of this loss, measures to prevent dangerous goods from being placed aboard aircraft were urgently recommended for airports which lacked sufficient security services.¹⁰⁶

¹⁰⁵ Wallis, *Combating Air Terrorism*, pp. 18-19.

¹⁰⁶ Exhibit P-448, p. 158.

April 5, 1988

A Kuwait Airways Boeing 747 aircraft, with 97 passengers and 15 crew on board, was seized by terrorists. The aircraft was diverted to Mashhad, Iran, where some hostages, including all the British passengers, were released, before the aircraft flew on to Cyprus. The Kuwaiti Government refused requests by the Iranian-backed Shia hijackers to release 17 convicted terrorists. Two passengers were killed while the aircraft was on the ground at Cyprus and the hijackers were allowed to fly to Algeria, where the remaining hostages were released unharmed and the terrorists were allowed to go free.¹⁰⁷

December 21, 1988

Pan Am Flight 103, a Boeing 747 aircraft, exploded over Lockerbie, Scotland. The cause was a bomb in an unaccompanied suitcase interlined to Pan Am at Frankfurt Airport in Germany. All 259 people on the aircraft and 11 people on the ground were killed by the blast. Abdelbasset Ali Mohmad Al- Megrahi, the Libyan Arab Airlines head of security and said to be a member of the Libyan Intelligence Service, was found guilty of the crime by a Scottish court sitting in the Hague.¹⁰⁸

1989

September 19,
1989¹⁰⁹

A French UTA DC-10 exploded in flight over the Sahara, killing all 171 persons on board. Plastic explosives had been hidden in a passenger's baggage.¹¹⁰ The bomb was believed to have been carried on board by a Congolese man who boarded the flight at Brazzaville in the Congo and disembarked at Ndjamena, a transit stop. It was thought that France's backing of elements opposed to the government of Libya and/or its support of anti-Syrian forces in Lebanon were the possible motivating factors behind this worst case of sabotage against a European airline.¹¹¹ The French government issued warrants for the arrest of four Libyans.¹¹²

¹⁰⁷ Exhibit P-35, p. 40; see also Wallis, *Combating Air Terrorism*, pp. 19-23,

¹⁰⁸ Exhibit P-35, p. 40; see also Wallis, *Combating Air Terrorism*, pp. 26-27.

¹⁰⁹ Exhibit P-448, p. 990.

¹¹⁰ Exhibit P-35, p. 41; see also Wallis, *Combating Air Terrorism*, pp. 39-40,

¹¹¹ Exhibit P-448, pp. 90-91.

¹¹² Exhibit P-35, p. 41; see also Wallis, *Combating Air Terrorism*, pp. 39-40,

November 1989	An Avianca Boeing 727 was destroyed on a domestic flight from Bogotá, Colombia, to Cali, killing 107. Persons with purported connections to a Colombian drug cartel claimed responsibility. ¹¹³
November 23, 1989	A loose wire is thought to have prevented the detonation of a bomb in the baggage compartment of Saudi Arabian Airlines Flight 367, a Boeing 747, which was flying over the Arabian Sea on a service from Islamabad, Pakistan, to Riyadh, Saudi Arabia. There were 339 persons on board. Ten passengers were subsequently arrested for their part in what appears to have been a suicide mission. ¹¹⁴
November 27, 1989	A Boeing 727 of Avianca was destroyed by an explosive device while flying between Bogotá, Colombia and Cali. All 107 persons on board died. The sabotage was believed to have been related to a drug cartel. ¹¹⁵
1994	
April 6, 1994	Rwandan president Juvenel Habyarimana was killed when his aircraft was shot down by a surface-to-air missile while approaching Kigali airport, Rwanda, on his return from a regional government leaders meeting. ¹¹⁶
July 19, 1994	A Middle East-related act of terrorism was suspected when an aircraft crashed near Colón, Panama, where it had taken off shortly before. All 21 persons on board were killed. ¹¹⁷

¹¹³ Wallis, *Combating Air Terrorism*, p. 41.

¹¹⁴ Exhibit P-448, p. 91.

¹¹⁵ Exhibit P-448, p. 160.

¹¹⁶ Exhibit P-35, p. 41.

¹¹⁷ Exhibit P-448, p. 92.

December 11, 1994

A bomb exploded under a seat in the cabin of a Philippine Airlines Boeing 747 flying from Manila, the Philippines, to Tokyo, Japan. The passenger occupying the seat was killed and 10 of the other 292 persons on board suffered injuries. The aircraft landed safely in Okinawa, Japan. This had reportedly been a “trial run” for a plan to blow up a dozen US airliners on trans-pacific flights, designed to punish the United States for its continued support of Israel. The principal saboteur in the plot was later convicted in a US court.¹¹⁸

December 24,
1994¹¹⁹

Air France Flight 8969, bound for Paris from Algiers, was hijacked by the Algerian terrorist organization Armed Islamic Group (GIA). The four hijackers boarded the aircraft disguised as Air Algérie security staff. Authorities delayed departure of the aircraft, but were intimidated into giving the go-ahead when the hijackers killed 2 of the 227 persons on board. The French government decided not to allow the aircraft to approach Paris because its consulate in Oran, Algeria, had received an intelligence warning that the hijackers intended to explode the aircraft over Paris. The flight crew convinced the hijackers that refueling in Marseille was required. After the aircraft touched down, hours of negotiations ensued, whereupon the terrorists demanded fuel. French police commandos (GIGN) stormed the aircraft and after a 20-minute gunfight successfully rescued the 161 remaining passengers (some had been released during negotiations) and 3 flight crew.¹²⁰

Conspirators smuggled improvised explosive device (IED) components through airport security and onto Philippine Airlines Flight 434, assembled them in the aircraft’s washroom and set the IED to detonate four hours later during the next leg of the flight. One person was killed and a hole was blown in the floor of the aircraft, which forced an emergency landing.¹²¹

118 Exhibit P-448, pp. 92-93.

119 Exhibit P-263, Tab 4.

120 Exhibit P-263, Tab 4.

121 Exhibit P-263, Tab 4.

1996

February 24, 1996	Two Cuban MiG fighters shot down a light aircraft flown by four Cuban exiles of the "Brothers to the Rescue" organization over the Gulf of Mexico. ¹²²
August, 1996	Six Iraqi dissidents hijacked a Sudan Airways A310 Airbus airliner en route from Khartoum to Jordan, diverting it to Stansted, UK. After negotiating with British authorities the hijackers released all 13 crew and 180 passengers unharmed. ¹²³
November 23, 1996	An Ethiopian Airways Boeing 767 was hijacked by three former prisoners while it was en route from Addis Ababa to Nairobi. The captain was ordered to fly the aircraft to Australia. It ran out of fuel and crashed into the Indian Ocean near the Comoros Islands killing 123 people. Fifty-two people, including 2 hijackers, survived. ¹²⁴

2001

September 11, 2001	Four US domestic passenger jets were hijacked and two of them were deliberately crashed into the towers of the New York World Trade Centre. Both buildings collapsed within an hour after the impacts. The third aircraft was deliberately flown into the side of the Pentagon building in Arlington, Virginia. The fourth aircraft crashed into the ground outside Pittsburgh, Pennsylvania. There were reports that this aircraft was headed for the White House. ¹²⁵ The total death toll was in the thousands.
--------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2003

March 4, 2003	A bomb hidden in a backpack exploded at an airport terminal in Davao in the southern Philippines, killing 21 people and wounding 148. ¹²⁶ The Moro Islamic Liberation Front (MILF) was suspected. ¹²⁷
---------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

¹²² Exhibit P-35, p. 41.

¹²³ Exhibit P-35, p. 41.

¹²⁴ Exhibit P-35, p. 41.

¹²⁵ Exhibit P-35, p. 42.

¹²⁶ Exhibit P-446.

¹²⁷ Exhibit P-447, p. 6.

November 22, 2003

A European Air Transport Airbus carrying 3 crew members was hit by a surface-to-air missile while climbing through 8,000 feet shortly after departure from Baghdad. The missile struck the wing, penetrating the no. 1A fuel tank and igniting the fuel. A large portion of the wing burned away. The aircraft landed safely. There were no casualties.¹²⁸

2006

August 10, 2006

An alleged terrorist plot to launch a simultaneous attack on a number of transatlantic flights was discovered in the United Kingdom. The threat was considered imminent and involved the alleged use of liquid and gel explosives concealed in carry-on baggage. A number of countries, including Canada, coordinated an immediate ban on all liquids and gels in carry-on baggage. The ban was eventually lifted in favour of allowing a restricted volume of liquids and gels in carry-on baggage, a pre-board screening measure which remains today.¹²⁹

2007

June 30, 2007

In what was determined to be a terrorist attack, a sports utility vehicle filled with gas canisters was driven into the front doors of the main terminal building of Glasgow Airport in Scotland and set ablaze.¹³⁰

¹²⁸ Criminal Occurrence Description (November 22, 2003), online: Aviation Safety Network <<http://aviation-safety.net/database/record.php?id=20031122-0>> (accessed January 26, 2010).

¹²⁹ See Testimony of Reg Whitaker, vol. 38, June 1, 2007, p. 4585; Testimony of Jean Barrette, vol. 39, June 4, 2007, p. 4842.

¹³⁰ Exhibit P-425, pp. 1-2 of 5.

APPENDIX B

Report on Security Arrangements Affecting Airports and Airlines in Canada

[“Seaborn Report”]

Principal Recommendations Of the Airport/Airline Security Report¹

1. The Department of Transport, Canadian Security Intelligence Service and the RCMP should ensure that they have the means to assess intelligence from all sources bearing on air security.
2. The Department should participate actively in the committee chaired by the Solicitor General’s departmental officials to review terrorist threat assessments and to ensure that users receive the required intelligence in a timely and usable manner.
3. The Department of Transport, the air carriers and interested associations should co-operate closely in the development of the security management system.
4. A graduated, multi-level system of security, with appropriate security measures for each level, will help to ensure swift and coherent responses to developing threat situations.
5. Airline personnel should not be exempt from security procedures in enhance[d] and high threat cases.
6. The Department of Transport must ensure that persons or materials introduced into international airports from other airfields are subject to the security standards in force at the international airport concerned.
7. The Department of Transport, the RCMP and the air carriers must ensure that the employees of private security firms performing security functions at airports meet prescribed security standards.
8. It would be desirable for all Canadian airside employees and others with regular access to particularly sensitive areas of the airport and to aircraft to be subject to security and criminal indices checks as a condition of employment.

¹ Exhibit P-101 CAF0039, pp. 9-10.

9. All workers at airports and the travelling public should be made aware of the contribution they can make to maintain a high level of air security.
10. The Minister of Transport and his Deputy should be responsible for ensuring that there is effective operation of all air security systems regardless of who may actually work them.
11. Significant decisions respecting security levels should be taken by the airport manager, senior departmental officials or the Minister, depending on the situation.
12. The Solicitor General should consult with the provincial Attorneys General to ensure that for each airport there is a police force designated that has the resources necessary to respond to acts of terrorism.
13. The Solicitor General and the appropriate Attorney General should pre-designate a commanding police officer who will have line authority over all airport, airline and other federal/provincial/municipal bodies that are likely to be involved in a terrorist incident. Under the *Security Offences Act* there is a presumption that this would be a member of the RCMP. This office should report through an agreed-on chain of command to the Solicitor General.
14. The Minister of Transport, in consultation with the Solicitor General, should report annually to the Prime Minister on the adequacy of the security regulations, the effectiveness with which they are applied, and the existence at each airport of an up-to-date "war book" for use in managing the response to terrorist incidents.
15. The Solicitor General should satisfy himself that, in the event of a terrorist threat or act, he is in a position to provide overall direction to those responsible for handling the crisis and to receive and disseminate information concerning such an event. He should test the mechanisms in place for this and report his findings to the Prime Minister.

APPENDIX C

The Myth of Security At Canada's Airports: Report of the Standing Senate Committee on National Security and Defence

Recommendations¹

Section I

- I.1 Transport Canada should, by March 31, 2003, finalize and issue training standards programs to equip cabin crews to deal with terrorists and/or terrorist materials. All flight crews should have completed training by September 30, 2003.
- I.2 The Canada Customs and Revenue Agency and Immigration Canada should, by June 30, 2003, offer substantive evidence to the Committee that they have addressed the Auditor General's recommendations to improve training that will help airport personnel identify persons "likely to engage in criminal activities or endanger the safety of Canadians." They should also demonstrate that they have made arrangements to gain access to police databanks that would assist in such identification, and have provided their employees with the training and technology required to take advantage of these databanks.
- I.3 Transport Canada should, by September 30, 2003, ensure that all Canadian passenger airlines are providing training courses to maintenance personnel and other personnel working in proximity to aircraft to help them identify potentially dangerous situations and materials.

Section II

- II.1 All flight crew should be informed when an Aircraft Protective Officer (APO) is on board.
- II.2 Transport Canada should, by June 30, 2003, require design completion of a double door system or systems to protect cockpits, and order air carriers to complete the installation of such systems by December 31, 2004.

¹ Exhibit P-171, pp. 143-149.

- II.3 APOs should be instructed by the RCMP to be prepared to intervene in violent disruptions in passenger cabins, and certainly be prepared to intervene if crew or passengers' lives are threatened, and not necessarily to restrain themselves until the very moment that any assault is launched on the cockpit.
- II.4 Pilots should not be armed.

Section III

- III.1 Dedicated and trained personnel should immediately begin carrying out random and targeted screening of all checked baggage, parcels, mailbags, and cargo.
- III.2 CATSA should implement full multi-layer screening (vapour detection supplemented by x-rays and other kinds of searches) of all checked baggage, mailbags and cargo by January 1, 2004.
- III.3 The practice of offering blanket security shortcuts on the basis of being a "known shipper" shipping by air carrier should be discontinued. The Committee encourages the development of a protocol for shippers based on their known reliability, similar to the one currently being introduced under the Smart Borders arrangement with the United States.
- III.4 People, cargo and aircraft coming from small airports without sophisticated screening systems should receive a full screening when they arrive at an airport under CATSA's jurisdiction.

Section IV

- IV.1 CATSA should issue national passes for air crew and all other persons who fall more naturally under a national, rather than a regional, jurisdiction. If local airport authorities are permitted to continue to issue passes allowing access to restricted areas at their airports, these local passes should be
 - Of national, uniform design, based on national configurations defined by the Canadian Air Transport Security Association,
 - Cancelable by CATSA
 - Validated through CATSA's national database.
- IV.2 All Canadian airports, by December 31, 2003, should introduce new electronic airside access passes, containing biometric identifiers, that
 - Are encoded to prevent access to zones beyond any employee's work area
 - Expire automatically after three years
 - Can be deactivated by a central control mechanism at any time

- IV.3 CATSA should be the issuing authority for passes for all employees, contract workers, other personnel and vehicles permitted airside access.
- IV.4 CATSA should be responsible for assuring that these persons and vehicles are physically searched on entry to restricted areas at Canada's airports. Persons and vehicles leaving those areas should be searched on a random basis, with provision for more extensive exit searches whenever extraordinary threats are perceived.
- IV.5 The current 5-point background check for restricted area passes: Canada Police Information Centre (for criminal record), CSIS (for potential security threats), and Transport Canada (domicile, employment background and credit records) should be conducted every three years, replacing the current schedule of every five years.

Section V

(This Recommendation repeated from Section IV)

- IV.4 CATSA should be responsible for assuring that these persons and vehicles are physically searched on entry to restricted areas at Canada's airports. Persons and vehicles leaving those areas should be searched on a random basis, with provision for more extensive exit searches whenever extraordinary threats are perceived.

This Recommendation Repeated from Section IV)

- IV.5 The current 5-point background check for restricted area passes: Canada Police Information Centre (for criminal record), CSIS (for potential security threats), and Transport Canada (domicile, employment background and credit records) should be conducted every three years, replacing the current schedule of every five years.

(This is a New Recommendation Contained Only in Section V)

- V.1 Transport Canada should require that private aircraft departing airports under CATSA's supervision should not leave until aircraft, passengers and their baggage have been screened. Private aircraft departing from any air facility not supervised by CATSA should be searched on arrival, whether they arrive from private air fields in Canada or any locations in foreign countries in order to ensure the integrity of security at Canadian airports.

Section VI

No recommendations at this time.

Section VII

- VII.1 All airport policing directly related to air travel security be removed from the airport authorities and assigned exclusively to the RCMP under contract to CATSA.
- VII.2 Local police forces and security guards contracted by airport authorities be responsible for criminal offences that are not related to air travel security.

Section VIII

- VIII.1 Transport Canada should continue to be responsible for the development of policy and standards for aircraft and airport security and should be responsible for verification that security policies are being implemented to its standards by CATSA, airport authorities, airlines, and police or other security personnel;
- VIII.2 CATSA should be responsible for the design and delivery of all mechanisms and training to assure air travel security, including the management and security screening of the restricted areas of the airport and the security screening of all persons and things boarding aircraft in Canada.
- VIII.3 National standards be effectively and consistently implemented. CATSA should develop an intelligence capability in order to effectively carry out its responsibilities.
- VIII.4 CATSA should be given the authority to contract the RCMP to supervise all policing at airports as it relates to passenger, cargo, aircraft and airside security.
- VIII.5 The Auditor General of Canada should conduct audits – including value for money audits – of security expenditures both by the federal government and airport authorities (the Minister of Transport should make this possible through new legislation.)

Section IX

- IX.1 The Government of Canada detail how much money is being collected from the \$12 air travellers security charge – better known as the departure tax – and from which airports;
- IX.2. The Government of Canada account for how much of the \$12 air travellers security charge, is being spent by CATSA, and how much is being spent by other departments and agencies and how much is being spent at each airport and for what;

- IX.3 That CATSA fully report the amounts that it is spending on its internal administration and report annually how much it has spent at each airport for: passenger screening, mail and cargo screening, airside searching of non-passengers, policing; and
- IX.4 That the Government of Canada introduce legislation providing the Auditor General of Canada with the power to audit each airport authority for accuracy, and value received for all security revenues and expenditures made by the authority, which would complement ongoing auditing and supervision by Transport Canada of security expenditures by airport authorities.

Section X

- X.1 The federal government should design and implement air travel security measures that provide transparency and full financial accountability to the Canadian public.
- X.2 Airport authorities and the airlines must recognize that security of air travel is the public's business and be forthright in explaining the measures they are taking to protect against terrorist or criminal activity, on the ground, and in the air.

APPENDIX D

Flight Plan: Managing the Risks in Aviation Security – Report of the Advisory Panel

List of Recommendations¹

CHAPTER ONE: REVIEWING CANADIAN AVIATION SECURITY

No recommendations.

CHAPTER TWO: PROTECTING CANADIAN AIR TRAVELERS

Recommendation 2.1

We recommend that responsibility for aviation security remain with the Minister of Transport.

Recommendation 2.2

Transport Canada should ensure that CATSA continues to receive all the information and intelligence it requires at the national and local levels to perform its functions, including timely access to the best intelligence and actionable information from all sources on explosives, weapons and concealment techniques.

Recommendation 2.3

Airports of all sizes should implement rigorous security awareness programs (a type of airport security watch program) for all personnel working at the airport.

Recommendation 2.4

We recommend that each designated airport establish an Airport Security Advisory Group, to coordinate and consult on the development and implementation of the airport's security plan, to resolve general security issues, to promote security awareness, and to encourage a collaborative approach to security issues.

¹ Exhibit P-169, pp. 173-179.

Recommendation 2.5

We recommend that an Airport Security Committee be created at each Class 1 airport to facilitate the sharing of intelligence information and to coordinate the development of airport-specific threat and risk assessments.

Recommendation 2.6

We recommend that Transport Canada accelerate its work to develop a program for the security screening of aviation cargo.

Recommendation 2.7

We recommend that screening of passengers be extended to Fixed Base Operations where the size of the operation warrants.

CHAPTER THREE: CATSA'S MANDATE

Recommendation 3.1

CATSA should retain its current screening mandates in the broadest sense of screening, that is, screening of people and things, and CATSA should be considered as the first option for all future aviation screening functions.

Recommendation 3.2

In Class 1 airports, CATSA should be continuously present at all entry points to the restricted areas of the airport to perform non-passenger screening, on a random basis.

- (a) Non-passenger screening should be extended to include searches of vehicles entering restricted areas in Class 1 airports, and should be performed by CATSA, or under CATSA's oversight using CATSA's standards and procedures.
- (b) Non-passenger screening should be discontinued in Class 2 airports once the Restricted Area Identification Card, with biometric identifiers, is in place; CATSA should be prepared to implement NPS on an as-needed basis in Class 2 and Class Other airports, when threat analysis indicates a need.

Recommendation 3.3

- (a) CATSA's mandate should be amended to remove responsibility for managing funding for the Canadian Air Carrier Protective Program. In the future, funding for the CACPP should be provided via appropriations directly to the RCMP or through Transport Canada.

- (b) An independent external audit of the CACPP should be conducted regularly by the Auditor General of Canada or an independent auditor, on a confidential basis.

Recommendation 3.4

- (a) Responsibility for the airport policing contribution program should be transferred to Transport Canada.
- (b) Transport Canada should review the existing standards for police response to all types of screening points to rationalize the airport policing program, and should fund all reasonable costs associated with meeting the new standards.

Recommendation 3.5

- (a) CATSA should complete the installation of the Restricted Area Identification Card system on a priority basis; to facilitate this, Transport Canada must complete the regulatory framework for RAIC as soon as possible.
- (b) Once CATSA has completed implementation of the Restricted Area Identification Card, the RAIC national identity verification system should be operated and maintained by Transport Canada.
- (c) The multiple-airport access system should be implemented in conjunction with RAIC as quickly as possible.
- (d) RAIC should be expanded to all 89 designated airports.

Recommendation 3.6

- (a) The text of the *CATSA Act* should be amended to remove the *consistency* criterion.
- (b) The text of the French version of the *CATSA Act* should be amended to add a separate term equivalent to *efficient* in section 6 (1).

CHAPTER FOUR: REGULATORY FRAMEWORK

Recommendation 4.1

It is recommended that CATSA develop a more user-friendly format for its *Standard Operating Procedures* and for disseminating and integrating updates to ensure that its front-line screening personnel have ready access to them in order to carry out their responsibilities.

Recommendation 4.2

Transport Canada should not retain the power to de-designate screening officers. CATSA should be accountable for screening officer performance, including certification and designation.

Recommendation 4.3

We recommend that to the extent possible, Transport Canada standardize the terminology used in the *Aeronautics Act*, its attendant regulations, measures and orders, and in the *CATSA Act*.

Recommendation 4.4

It is recommended that, as a high priority, Transport Canada develop a more results-based regulatory framework for aviation security.

Recommendation 4.5

It is recommended that, in line with ICAO Annex 17, Transport Canada develop a National Civil Aviation Security Program and require CATSA, as well as airport operators, major tenants and air carriers, to develop security plans for their areas of responsibility, consistent with the National Program. Transport Canada should approve the plans and audit the organizations on a periodic basis for compliance with their plans.

Recommendation 4.6

In line with the results-based regulatory regime, it is recommended that CATSA assume full responsibility (and accountability) for operational policy, including operational design and screening solutions, qualifications of screening officers and service providers, equipment decisions and management of the list of prohibited items.

CHAPTER FIVE: DELIVERY OF SCREENING SERVICES**Recommendation 5.1**

- (a) All three options for CATSA to deliver screening services should remain in the *CATSA Act*.
- (b) Airport operators should be eligible to bid on a screening contract for their own airport.

Recommendation 5.2

- (a) CATSA should develop measurable performance standards, including peak hour throughput and wait-time standards for each airport that reflect, among other factors, the pre-board screening configuration at the various screening points.
- (b) CATSA should establish space allocation standards for pre-board screening lines and a throughput standard for an optimum configuration.
- (c) CATSA should develop workplace design standards to optimize screening effectiveness and employee working conditions and ensure best practices are shared with all airports.

Recommendation 5.3

We recommend that CATSA provide refresher courses to screening officers on new screening techniques, and changes to the *CATSA Standard Operating Procedures*, to ensure that screening officers maintain an up-to-date knowledge of their complete content.

Recommendation 5.4

CATSA should consider options to improve supervision at all 89 airports. CATSA should deploy more management personnel in the field in order to provide closer supervision of security screening services.

Recommendation 5.5

As a high priority, Transport Canada, CATSA, airport operators, air carriers and police services must develop unambiguous guidelines on the handling of security breach incidents at all screening points. These guidelines should include clear and timely communications to the public.

Recommendation 5.6

We recommend that Transport Canada undertake a detailed audit of the security clearance process to determine the causes of delay, and take remedial action to correct these deficiencies, in order to speed up the process of issuing Transportation Security Clearances for persons requiring airport Restricted Area Passes.

CHAPTER SIX: GOVERNANCE AND ACCOUNTABILITY

Recommendation 6.1

We recommend that CATSA establish a national-level advisory committee, reporting to the Board of Directors, to represent the interests of the travelling public, including travellers with disabilities.

Recommendation 6.2

- (a) It is recommended that the Canadian Air Transport Security Authority either remain a Crown corporation or be transformed into a departmental corporation.
- (b) If CATSA remains a Crown corporation, there should be an increase in the level of compensation provided to Board members.
- (c) If CATSA becomes a departmental corporation, an advisory board representing the various stakeholders should be established. The Minister should appoint its members.

Recommendation 6.3

Whichever organizational model is adopted for CATSA, the organization needs to be provided with increased flexibility in the areas of operations, finance and administration.

Recommendation 6.4

- (a) In order to carry out its mandate effectively, CATSA should be responsible and accountable for operational policy and decisions (including deployment of human resources and the lifecycle management of its assets), while Transport Canada would retain responsibility for overall aviation security policy, strategy and legislation.
- (b) These responsibilities and accountabilities should be clearly communicated at all levels of both organizations, and their acceptance needs to be carefully monitored.

Recommendation 6.5

CATSA should have full responsibility for the lifecycle management of its capital equipment, including research and development, procurement, maintenance and replacement.

Recommendation 6.6

We recommend that CATSA's budget reflect passenger volumes as well as productivity gains realized from enhanced technologies and procedures. CATSA should also be provided with the capacity to generate revenues, to recover costs in line with federal government policies, to carry forward operating funds, to re-profile capital and to transfer operating funds between budget items. These flexibilities should be awarded once CATSA has demonstrated it has the appropriate procedures and systems in place.

Recommendation 6.7

We recommend that, if CATSA becomes a departmental corporation, it remain a separate employer, be granted the same contracting authorities that it has as a Crown corporation and the maximum administrative flexibilities allowed for under the *Financial Administration Act*.

CHAPTER SEVEN: FUTURE AVIATION SECURITY IMPLICATIONS

Recommendation 7.1

We recommend that Transport Canada and CATSA take steps to instill a culture of continuous learning from past events and forward-looking threat assessment throughout their organizations, and in collaboration with other security partners.

Recommendation 7.2

It is recommended that CATSA have responsibility for the assessment (including pilot projects) of emerging technologies and techniques in the detection of potential threats, as part of its lifecycle management of its capital program.

CHAPTER EIGHT: OTHER OBSERVATIONS

No recommendations.

APPENDIX E

Canadian Security Guide Book 2007 Edition - Airports

APPENDIX III¹

Index of New Recommendations

Problem 1(a): Insufficient Airport Policing

- A1. The Committee recommends that the Government of Canada increase the size of the RCMP by between 600 and 800 full-time equivalents (FTEs) in order to provide the RCMP with the capacity to:
- Execute a new mandate of oversight and responsibility for security at airports and,
 - Expand its investigative and analytical capabilities at airports within the National Airport System.
- A2. The Committee recommends that Public Safety and Emergency Preparedness Canada conduct tests to ascertain the level of cooperation of multiple police forces operating at major Canadian airports. These tests should be conducted within the next year, and the results should be made public and recommendations acted upon six months after they are issued.

Problem 1(b): Inadequate Background Checks

- A3. The Committee recommends that the ratio of airport employees with background checks/pass escorting or supervising employees without background checks/pass be 1 to 5.

Problem 1(c): Inadequate Control of Access to Restricted Areas

- A4. The Committee recommends that the level of random checking on departure be set at a minimum of 10 percent daily, or at a higher level so as to ensure that the smuggling of contraband is deterred.
- A5. The Committee recommends that by December 31, 2008 airport restricted area identification cards should be augmented with geofencing to detect irregular employee behaviour.

Problem 2: Checking the Legitimacy of Flight Crews and Ground Crew

No change – see Appendix II

¹ Exhibit P-172, pp. 91-94.

Problem 3: Unscreened Airmail and Other Cargo

No change – see Appendix II

Problem 4: Screening Checked Baggage

A6. The Committee recommends that since all passengers are searched for liquids, gels and weapons, all materials being loaded onto aircrafts should also be checked for weapons and potentially volatile liquids and gels, which in combination could be explosive. This includes searching airline catering service carts.

Problem 5: Vulnerable Cockpit Doors

- A7. The Committee recommends that all future aircraft used by Canadian airlines should be outfitted with a comprehensive bulletproof divider between the cockpit and the cabin.
- A7a. The Committee recommends that once these dividers are installed, the use of Aircraft Protection Officers (APO) should be discontinued on all flights other than flights to Reagan Airport in Washington.
- A7b. The cost of APOs on flights to Reagan should be incurred by the airlines, not Canadian taxpayers.

Problem 6: Alerting Air Crews

- A8. The Committee recommends that as long as the Aircraft Protection Officer program exists, Transport Canada make it a requirement that all crew members be briefed as to who the APOs are, their seat location, and how the crew is expected to respond in the event of an attempted hijacking.

Problem 7: Security Training for Maintenance Workers

No change – see Appendix II

Problem 8: Who's In Charge of Security at Canadian Airports?

- A9. The Committee recommends that Transport Canada be relieved of its responsibility for security at airports and that this responsibility be transferred to the Department of Public Safety and Emergency Preparedness Canada.

Problem 9: “Known Shipper” System Lessens Aircraft Security

- A10. The Committee recommends that the Government of Canada take the appropriate steps to expedite this study on air cargo security to bring forth results by Spring 2008.
- A11. The Committee recommends that the Government of Canada use the results of the study to create a fail-safe system that will fill the gaps in air cargo security within a year after the study’s results are identified.

Problem 10: Lack of Security at Fixed-Base Operations

- A12. The Committee recommends that all individuals and vehicles, including private aircrafts, be searched at all fixed-base operations that are attached to the current 89 designated airports.
- A12a. The Committee recommends that aviation facilities in the core of municipalities such as Victoria and Vancouver be immediately designated for CATSA supervision.

Problem 11: Small Airports are Weak Links in the Aviation Security Net

No change – see Appendix II

Problem 12: The Canadian Air Transport Security Intelligence Gap

- A13. The Committee recommends that the Government of Canada ensure that CATSA has access to all available intelligence related to aviation safety.
- A14. The Committee recommends that in partnership with the RCMP and CSIS, CATSA develop its own intelligence analysis capabilities.

Problem 13: Unnecessary Secrecy over Security

- A15. The Committee recommends that the Government of Canada make public results of “intrusion tests” within six months of the tests being conducted by the airport, or that the Government of Canada put into effect a plan that would make the results public on a regular basis after a longer, but reasonable, period so that it has sufficient time to remedy the deficiencies uncovered by the tests.

Problem 14: Air Travellers Security Charge

No change – see Appendix II

Problem 15: Lack of Transparency over Security Expenditures Generally

- A16. The Committee recommends that the Government of Canada invite the Auditor General of Canada to conduct a “Value-for-money” audit on security expenditures such as the Air Traveller Security Charge to ensure that the money collected from passengers is in fact going to technologies and activities that are protecting them effectively.

